Honeywell

THE POWER OF **CONNECTED**

Microsoft® Windows Patches Tested with MAXPRO®NVR and MAXPRO®VMS

The purpose of this document is to identify the patches that have been delivered by Microsoft® Windows and which have been tested against the current shipping versions of MAXPRO®NVR and MAXPRO®VMS with no adverse effects being observed.

If you have questions concerning the information in this document, please contact Honeywell Technical Support. See the back cover for contact information.

Windows Patches Tested with MAXPRO®NVR till the Month of: October, 2017

Windows Patches Tested with MAXPRO®VMS till the Month of: October, 2017

This document contains:

MAXPRO® NVR Current Shipping Version

- MAXPRO® NVR (Server and Client) R4.0 Build 87 Rev H + 4.1.0.97 + R4.1 Build 123 Rev B (on Windows Embedded Standard SP1)

MAXPRO® VMS Current Shipping Version

- MAXPRO® VMS Server 4.10.0.424 Build 424 (on Windows Server 2012 R2 Standard 64 bit Server)
- MAXPRO® VMS Client 4.10.0.424 Build 424 (on Windows 10 Pro 64 bit Client)

MAXPRO® NVR: Windows Patches Tested with Microsoft® Windows OS

- Microsoft® Windows Embedded Standard 7 SP1, 32-bit / 64-bit

MAXPRO® VMS: Windows Patches Tested with Microsoft® Windows OS

- Microsoft® Windows 10 Professional, 32-bit / 64-bit
- Microsoft Windows 2012 R2 Standard 64 bit Server.

October - 2017- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

Microsoft Knowledge Base Article ID	Description
KB4040685	**Cumulative security update for Internet Explorer: October 10, 2017**
KB4041678	**This security update includes quality improvements. No new operating system features are being introduced in this update**
KB2533552	**An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available**
KB976932	**Information about Service Pack 1 for Windows 7 and for Windows Server 2008 R2**
KB4041681	**This security update includes improvements and fixes that were a part of update KB4038803 (released September 19, 2017)**
KB4041687	**October 10, 2017—KB4041687 (Security-only update)**
KB4041693	**This security update includes improvements and fixes that were a part of update KB4038774**

Microsoft Knowledge Base Article ID	Description
KB3125217	Disk cleanup for Windows 10 cumulative updates
KB3172729	MS16-100: Description of the security update for Secure Boot
KB3173427	Servicing stack update for Windows 10
KB4022730	Security update for Adobe Flash Player
KB4022727	This security update includes quality improvements. No new operating system features are being introduced in this update

September - 2017- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

Microsoft Knowledge Base Article ID	Description
KB4036586	Cumulative security update for Internet Explorer: September 12, 2017
KB4038779	This security update includes quality improvements. No new operating system features are being introduced in this update. September 12, 2017—KB4038779 (Security-only update)
KB4040980	Description of the Security and Quality Rollup for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1: September 12, 2017
KB4038777	This security update includes improvements and fixes that were a part of update KB4034670 (released August 15, 2017)
KB4038793	This security update includes quality improvements. No new operating system features are being introduced in this update September 12, 2017—KB4038793 (Security-only update)
KB4038806	S ecurity update for Adobe Flash Player: September 12, 2017
KB4040956	Description of the Security Only update for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2: September 12, 2017
KB4040967	Description of the Security Only update for the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 12, 2017
KB4040972	Description of the Security and Quality Rollup for the .NET Framework 4.6, 4.6.1, 4.6.2 and 4.7 for Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2: September 12, 2017

Microsoft Knowledge Base Article ID	Description
KB4040981	Description of the Security and Quality Rollup for the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: September 12, 2017
KB4038774	This non-security update includes improvements and fixes that were a part of KB4038792 (released September 12, 2017). September 19, 2017—KB4038774 (Preview of Monthly Rollup)
KB4040724	This update includes quality improvements. No new operating system features are being introduced in this update September 25, 2017—KB4040724 (OS Build 15063.632)

August - 2017- Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

Microsoft KnowledgeBase Article ID	Description
KB4034674	August 8, 2017—KB4034674 (OS Build 15063.540)
KB4034663	August 15, 2017—KB4034663 (Preview of Monthly Rollup)
KB4034662	Security update for Adobe Flash Player: August 8, 2017
KB4033997	Description of Preview of Quality Rollup for the .NET Framework 3.5 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: August 15, 2017
KB4033989	Description of Preview of Quality Rollup for the .NET Framework 4.6, 4.6.1, 4.6.2, and 4.7 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2: August 15, 2017
KB4034664	August 8, 2017—KB4034664 (Monthly Rollup)
KB4033996	Description of Preview of Quality Rollup for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1: August 15, 2017

2017 -Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

2016 -Microsoft® Windows Patches Tested with MAXPRO®VMS/NVR

Microsoft KnowledgeBase Article ID	Description
KB4025341	July 11, 2017—KB4025341 (Monthly Rollup)
KB4033428	Windows Server 2012 R2 processor generation detection reliability update: July 18, 2017
KB4025335	July 18, 2017—KB4025335 (Preview of Monthly Rollup)
KB4025339	July 11, 2017—KB4025339 (OS Build 14393.1480)
KB4025376	Security update for Adobe Flash Player: July 11, 2017
KB4022719	June 13, 2017—KB4022719 (Monthly Rollup). This security update includes improvements and fixes that were a part of update KB4019265 (released May 16, 2017)
KB3186539	The Microsoft .NET Framework 4.7 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2
KB4022726	June 13, 2017—KB4022726 (Monthly Rollup) This security update includes improvements and fixes that were a part of update ?KB4019217 (released May 16th, 2017)
KB4022715	June 13, 2017—KB4022715 (OS Build 14393.1358) This security update includes quality improvements. No new operating system features are being introduced in this update.
KB4023834	Servicing Stack Update for Windows 10 1607 and Windows Server 2016: June 13, 2017
KB4022730	Security update for Adobe Flash Player: June 13, 2017
KB3186568	The Microsoft .NET Framework 4.7 for Windows 10 Version 1607 and Windows Server 2016
KB4019990	Update for the d3dcompiler_47.dll component on Windows Server 2012, Windows 7, and Windows Server 2008 R2
KB4014596	May 2017 Description of the Quality Rollup for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1 (KB4014596): May 16, 2017
KB4019472	May 9, 2017—KB4019472 (OS Build 14393.1198)
KB3150513	Latest compatibility definition update for Windows
KB4019264	May 9, 2017—KB4019264 (Monthly Rollup)
KB4014504	Description of the Security and Quality Rollup for the .NET Framework 3.5.1 for Windows 7 and Windows Server 2008 R2: May 9, 2017
KB4019217	May 16, 2017—KB4019217 (Preview of Monthly Rollup)
KB4020821	Security update for Adobe Flash Player: May 9, 2017
KB4014604	May 2017 Description of the Quality Rollup for the .NET Framework 4.6, 4.6.1, and 4.6.2 for Windows 8.1 and Windows Server 2012 R2 (KB4014604): May 16, 2017
KB4014598	May 2017 Description of the Quality Rollup for the .NET Framework 3.5 for Windows 8.1 and Windows Server 2012 R2 (KB4014598): May 16, 2017
KB4014510	Description of the Security and Quality Rollup for the .NET Framework 4.6 and 4.6.1 for Windows 8.1 and Windows Server 2012 R2: May 9, 2017

Microsoft KnowledgeBase Article ID	Description
KB4014505	Description of the Security and Quality Rollup for the .NET Framework 3.5 Service Pack 1 for Windows 8.1 and Windows Server 2012 R2: May 9, 2017
KB4012219	March 2017 Preview of Monthly Quality Rollup for Windows 8.1 and Windows Server 2012 R2
KB4015438	This update includes quality improvements. No new operating system features are being introduced in this update.
KB4013418	This update makes stability improvements for the Windows 10 Version 1607 and Windows Server 2016 servicing stack.
KB4012215	March 2017 Security Monthly Quality Rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1
MS17-023	Security Update for Adobe Flash Player (4014329)
MS17-022	Security Update for Microsoft XML Core Services (4010321)
MS17-021	Security Update for Windows DirectShow (4010318)
MS17-020	Security Update for Windows DVD Maker (3208223)
MS17-019	Security Update for Active Directory Federation Services (4010320)
MS17-018	Security Update for Windows Kernel-Mode Drivers (4013083)
MS17-017	Security Update for Windows Kernel (4013081)
MS17-016	Security Update for Windows IIS (4013074)
MS17-015	Security Update for Microsoft Exchange Server (4013242)
MS17-014	Security Update for Microsoft Office (4013241)
MS17-013	Security Update for Microsoft Graphics Component (4013075)
MS17-012	Security Update for Microsoft Windows (4013078)
MS17-011	Security Update for Microsoft Uniscribe (4013076)
MS17-010	Security Update for Microsoft Windows SMB Server (4013389)
MS17-009	Security Update for Microsoft Windows PDF Library (4010319)
MS17-008	Security Update for Windows Hyper-V (4013082)
MS17-007	Cumulative Security Update for Microsoft Edge (4013071)
MS17-006	Cumulative Security Update for Internet Explorer (4013073)
MS17-005	Security Update for Adobe Flash Player (4010250)
MS17-004	Security Update for Local Security Authority Subsystem Service (3216771)
MS17-003	Security Update for Adobe Flash Player (3214628)
MS17-002	Security Update for Microsoft Office (3214291)
MS17-001	Security Update for Microsoft Edge (3214288)

Microsoft KnowledgeBase Article ID	Description
KB3211320	Servicing stack update for Windows 10 Version 1607 and Windows Server 2016: January 24, 2017
KB4009938	January 10, 2017—KB3213986 (OS Build 14393.693)
KB3212646	January 2017 Security Monthly Quality Rollup for Windows 7 SP1 and Windows Server 2008 R2 SP1

Microsoft KnowledgeBase Article ID	Description
MS16-155	Security Update for .NET Framework (3205640)
MS16-154	Security Update for Adobe Flash Player (3209498)
MS16-153	Security Update for Common Log File System Driver (3207328)
MS16-152	Security Update for Windows Kernel (3199709)
MS16-151	Security Update for Windows Kernel-Mode Drivers (3205651)
MS16-150	Security Update for Secure Kernel Mode (3205642)
MS16-149	Security Update for Microsoft Windows (3205655)
MS16-148	Security Update for Microsoft Office (3204068)
MS16-147	Security Update for Microsoft Uniscribe (3204063)
MS16-146	Security Update for Microsoft Graphics Component (3204066)
MS16-145	Cumulative Security Update for Microsoft Edge (3204062)
MS16-144	Cumulative Security Update for Internet Explorer (3204059)
MS16-142	Cumulative Security Update for Internet Explorer (3198467)
MS16-141	Security Update for Adobe Flash Player (3202790)
MS16-140	Security Update for Boot Manager (3193479)
MS16-139	Security Update for Windows Kernel (3199720)
MS16-138	Security Update to Microsoft Virtual Hard Disk Driver (3199647)
MS16-137	Security Update for Windows Authentication Methods (3199173)
MS16-136	Security Update for SQL Server (3199641)
MS16-135	Security Update for Windows Kernel-Mode Drivers (3199135)
MS16-134	Security Update for Common Log File System Driver (3193706)
MS16-133	Security Update for Microsoft Office (3199168)
MS16-132	Security Update for Microsoft Graphics Component (3199120)
MS16-131	Security Update for Microsoft Video Control (3199151)
MS16-130	Security Update for Microsoft Windows (3199172)

Microsoft KnowledgeBase Article ID	Description
MS16-129	Cumulative Security Update for Microsoft Edge (3199057)
MS16-128	Security Update for Adobe Flash Player (3201860)
MS16-127	Security Update for Adobe Flash Player (3194343)
MS16-126	Security Update for Microsoft Internet Messaging API (3196067)
MS16-125	Security Update for Diagnostics Hub (3193229)
MS16-124	Security Update for Windows Registry (3193227)
MS16-123	Security Update for Windows Kernel-Mode Drivers (3192892)
MS16-122	Security Update for Microsoft Video Control (3195360)
MS16-121	Security Update for Microsoft Office (3194063)
MS16-120	Security Update for Microsoft Graphics Component (3192884)
MS16-119	Cumulative Security Update for Microsoft Edge (3192890)
MS16-118	Cumulative Security Update for Internet Explorer (3192887)
MS16-117	Security Update for Adobe Flash Player (3188128)
MS16-116	Security Update in OLE Automation for VBScript Scripting Engine (3188724)
MS16-115	Security Update for Microsoft Windows PDF Library (3188733)
MS16-114	Security Update for SMBv1 Server (3185879)
MS16-113	Security Update for Windows Secure Kernel Mode (3185876)
MS16-112	Security Update for Windows Lock Screen (3178469)
MS16-111	Security Update for Windows Kernel (3186973)
MS16-110	Security Update for Windows (3178467)
MS16-109	Security Update for Silverlight (3182373)
MS16-108	Security Update for Microsoft Exchange Server (3185883)
MS16-107	Security Update for Microsoft Office (3185852)
MS16-106	Security Update for Microsoft Graphics Component (3185848)
MS16-105	Cumulative Security Update for Microsoft Edge (3183043)
MS16-104	Cumulative Security Update for Internet Explorer (3183038)

2016 - Microsoft® Windows Patches Tested with MAXPRO®NVR

Microsoft KnowledgeBase Article ID	Description
MS16-103	Security Update for ActiveSyncProvider (3182332)
MS16-102	Security Update for Microsoft Windows PDF Library (3182248)
MS16-101	Security Update for Windows Authentication Methods (3178465)
MS16-100	Security Update for Secure Boot (3179577)
MS16-099	Security Update for Microsoft Office (3177451)
MS16-098	Security Update for Windows Kernel-Mode Drivers (3178466)
MS16-097	Security Update for Microsoft Graphics Component (3177393)
MS16-096	Cumulative Security Update for Microsoft Edge (3177358)
MS16-095	Cumulative Security Update for Internet Explorer (3177356)
MS16-094	Security Update for Secure Boot (3177404)
MS16-093	Security Update for Adobe Flash Player (3174060)
MS16-092	Security Update for Windows Kernel (3171910)
MS16-091	Security Update for .NET Framework (3170048)
MS16-090	Security Update for Windows Kernel-Mode Drivers (3171481)
MS16-089	Security Update for Windows Secure Kernel Mode (3170050)
MS16-088	Security Update for Microsoft Office (3170008)
MS16-087	Security Update for Windows Print Spooler Components (3170005)
MS16-086	Cumulative Security Update for JScript and VBScript (3169996)
MS16-085	Cumulative Security Update for Microsoft Edge (3169999)
MS16-084	Cumulative Security Update for Internet Explorer (3169991)
MS16-083	Security Update for Adobe Flash Player (3167685)
MS16-082	Security Update for Microsoft Windows Search Component (3165270)
MS16-081	Security Update for Active Directory (3160352)
MS16-080	Security Update for Microsoft Windows PDF (3164302)
MS16-079	Security Update for Microsoft Exchange Server (3160339)
MS16-078	Security Update for Windows Diagnostic Hub (3165479)
MS16-077	Security Update for WPAD (3165191)
MS16-076	Security Update for Netlogon (3167691)
MS16-075	Security Update for Windows SMB Server (3164038)
MS16-074	Security Update for Microsoft Graphics Component (3164036)
MS16-073	Security Update for Windows Kernel-Mode Drivers (3164028)

Microsoft KnowledgeBase Article ID	Description
MS16-072	Security Update for Group Policy (3163622)
MS16-071	Security Update for Microsoft Windows DNS Server (3164065)
MS16-070	Security Update for Microsoft Office (3163610)
MS16-069	Cumulative Security Update for JScript and VBScript (3163640)
MS16-068	Cumulative Security Update for Microsoft Edge (3163656)
MS16-067	Security Update for Volume Manager Driver (3155784)
MS16-066	Security Update for Virtual Secure Mode (3155451)
MS16-065	Security Update for .NET Framework (3156757)
MS16-064	Security Update for Adobe Flash Player (3157993)
MS16-063	Cumulative Security Update for Internet Explorer (3163649)
MS16-062	Security Update for Windows Kernel-Mode Drivers (3158222)
MS16-061	Security Update for Microsoft RPC (3155520)
MS16-060	Security Update for Windows Kernel (3154846)
MS16-059	Security Update for Windows Media Center (3150220)
MS16-058	Security Update for Windows IIS (3141083)
MS16-057	Security Update for Windows Shell (3156987)
MS16-056	Security Update for Windows Journal (3156761)
MS16-055	Security Update for Microsoft Graphics Component (3156754)
MS16-054	Security Update for Microsoft Office (3155544)
MS16-053	Cumulative Security Update for JScript and VBScript (3156764)
MS16-052	Cumulative Security Update for Microsoft Edge (3155538)
MS16-051	Cumulative Security Update for Internet Explorer (3155533)
MS16-050	Security Update for Adobe Flash Player (3154132)
MS16-049	Security Update for HTTP.sys (3148795)
MS16-048	Security Update for CSRSS (3148528)
MS16-047	Security Update for SAM and LSAD Remote Protocols (3148527)
MS16-046	Security Update for Secondary Logon (3148538)
MS16-045	Security Update for Windows Hyper-V (3143118)
MS16-044	Security Update for Windows OLE (3146706)
MS16-042	Security Update for Microsoft Office (3148775)
MS16-041	Security Update for .NET Framework (3148789)
MS16-040	Security Update for Microsoft XML Core Services (3148541)

Microsoft KnowledgeBase Article ID	Description
MS16-039	Security Update for Microsoft Graphics Component (3148522)
MS16-038	Cumulative Security Update for Microsoft Edge (3148532)
MS16-037	Cumulative Security Update for Internet Explorer (3148531)
MS16-036	Security Update for Adobe Flash Player (3144756)
MS16-035	Security Update for .NET Framework to Address Security Feature Bypass (3141780)
MS16-034	Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3143145)
MS16-033	Security Update for Windows USB Mass Storage Class Driver to Address Elevation of Privilege (3143142)
MS16-032	Security Update for Secondary Logon to Address Elevation of Privilege (3143141)
MS16-031	Security Update for Microsoft Windows to Address Elevation of Privilege (3140410)
MS16-030	Security Update for Windows OLE to Address Remote Code Execution (3143136)
MS16-029	Security Update for Microsoft Office to Address Remote Code Execution (3141806)
MS16-028	Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3143081)
MS16-027	Security Update for Windows Media to Address Remote Code Execution (3143146)
MS16-026	Security Update for Graphic Fonts to Address Remote Code Execution (3143148)
MS16-025	Security Update for Windows Library Loading to Address Remote Code Execution (3140709)
MS16-024	Cumulative Security Update for Microsoft Edge (3142019)
MS16-023	Cumulative Security Update for Internet Explorer (3142015)
MS16-022	Security Update for Adobe Flash Player (3135782)
MS16-021	Security Update for NPS RADIUS Server to Address Denial of Service (3133043)
MS16-020	Security Update for Active Directory Federation Services to Address Denial of Service (3134222)
MS16-019	Security Update for .NET Framework to Address Denial of Service (3137893)
MS16-018	Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3136082)
MS16-017	Security Update for Remote Desktop Display Driver to Address Elevation of Privilege (3134700)
MS16-016	Security Update for WebDAV to Address Elevation of Privilege (3136041)
MS16-015	Security Update for Microsoft Office to Address Remote Code Execution (3134226)
MS16-014	Security Update for Microsoft Windows to Address Remote Code Execution (3134228)
MS16-013	Security Update for Windows Journal to Address Remote Code Execution (3134811)

Microsoft KnowledgeBase Article ID	Description
MS16-012	Security Update for Microsoft Windows PDF Library to Address Remote Code Execution (3138938)
MS16-011	Cumulative Security Update for Microsoft Edge (3134225)
MS16-010	Security Update in Microsoft Exchange Server to Address Spoofing (3124557)
MS16-009	Cumulative Security Update for Internet Explorer (3134220)
MS16-008	Security Update for Windows Kernel to Address Elevation of Privilege (3124605)
MS16-007	Security Update for Microsoft Windows to Address Remote Code Execution (3124901)
MS16-006	Security Update for Silverlight to Address Remote Code Execution (3126036)
MS16-005	Security Update for Windows Kernel-Mode Drivers to Address Remote Code Execution (3124584)
MS16-004	Security Update for Microsoft Office to Address Remote Code Execution (3124585)
MS16-003	Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3125540)
MS16-002	Cumulative Security Update for Microsoft Edge (3124904)
MS16-001	Cumulative Security Update for Internet Explorer (3124903)

2015 - Microsoft® Windows Patches Tested with MAXPRO®NVR

Microsoft KnowledgeBase Article ID	Description
MS15-135	Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3119075)
MS15-134	Security Update for Windows Media Center to Address Remote Code Execution (3108669)
MS15-133	Security Update for Windows PGM to Address Elevation of Privilege (3116130)
MS15-132	Security Update for Microsoft Windows to Address Remote Code Execution (3116162)
MS15-131	Security Update for Microsoft Office to Address Remote Code Execution (3116111)
MS15-130	Security Update for Microsoft Uniscribe to Address Remote Code Execution (3108670)
MS15-129	Security Update for Silverlight to Address Remote Code Execution (3106614)
MS15-128	Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)
MS15-127	Security Update for Microsoft Windows DNS to Address Remote Code Execution (3100465)
MS15-126	Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3116178)
MS15-125	Cumulative Security Update for Microsoft Edge (3116184)
MS15-124	Cumulative Security Update for Internet Explorer (3116180)
MS15-123	Security Update for Skype for Business and Microsoft Lync to Address Information Disclosure (3105872)
MS15-122	Security Update for Kerberos to Address Security Feature Bypass (3105256)
MS15-121	Security Update for Schannel to Address Spoofing (3081320)
MS15-120	Security Update for IPSec to Address Denial of Service (3102939)
MS15-119	Security Update for Winsock to Address Elevation of Privilege (3104521)
MS15-118	Security Update for .NET Framework to Address Elevation of Privilege (3104507)
MS15-117	Security Update for NDIS to Address Elevation of Privilege (3101722)
MS15-116	Security Update for Microsoft Office to Address Remote Code Execution (3104540)
MS15-115	Security Update for Microsoft Windows to Address Remote Code Execution (3105864)
MS15-114	Security Update for Windows Journal to Address Remote Code Execution (3100213)
MS15-113	Cumulative Security Update for Microsoft Edge (3104519)
MS15-112	Cumulative Security Update for Internet Explorer (3104517)
MS15-111	Security Update for Windows Kernel to Address Elevation of Privilege (3096447)
MS15-110	Security Updates for Microsoft Office to Address Remote Code Execution (3096440)
MS15-109	Security Update for Windows Shell to Address Remote Code Execution (3096443)

MS15-108	Security Update for JScript and VBScript to Address Remote Code Execution (3089659)
MS15-107	Cumulative Security Update for Microsoft Edge (3096448)
MS15-106	Cumulative Security Update for Internet Explorer (3096441)
MS15-105	Vulnerability in Windows Hyper-V Could Allow Security Feature Bypass (3091287)
MS15-104	Vulnerabilities in Skype for Business Server and Lync Server Could Allow Elevation of Privilege (3089952)
MS15-103	Vulnerabilities in Microsoft Exchange Server Could Allow Information Disclosure (3089250)
MS15-102	Vulnerabilities in Windows Task Management Could Allow Elevation of Privilege (3089657)
MS15-101	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3089662)
MS15-100	Vulnerability in Windows Media Center Could Allow Remote Code Execution (3087918)
MS15-099	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3089664)
MS15-098	Vulnerabilities in Windows Journal Could Allow Remote Code Execution (3089669)
MS15-097	Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3089656)
MS15-096	Vulnerability in Active Directory Service Could Allow Denial of Service (3072595)
MS15-095	Cumulative Security Update for Microsoft Edge (3089665)
MS15-094	Cumulative Security Update for Internet Explorer (3089548)
MS15-093	Security Update for Internet Explorer (3088903)
MS15-092	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3086251)
MS15-091	Cumulative Security Update for Microsoft Edge (3084525)
MS15-090	Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3060716)
MS15-089	Vulnerability in WebDAV Could Allow Information Disclosure (3076949)
MS15-088	Unsafe Command Line Parameter Passing Could Allow Information Disclosure (3082458)
MS15-087	Vulnerability in UDDI Services Could Allow Elevation of Privilege (3082459)
MS15-086	Vulnerability in System Center Operations Manager Could Allow Elevation of Privilege (3075158)
MS15-085	Vulnerability in Mount Manager Could Allow Elevation of Privilege (3082487)
MS15-084	Vulnerabilities in XML Core Services Could Allow Information Disclosure (3080129)
MS15-083	Vulnerability in Server Message Block Could Allow Remote Code Execution (3073921)
MS15-082	Vulnerabilities in RDP Could Allow Remote Code Execution (3080348)
MS15-081	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3080790)
MS15-080	Vulnerabilities in Microsoft Graphics Component Could Allow Remote Code Execution (3078662)
MS15-079	Cumulative Security Update for Internet Explorer (3082442)

MS15-078	**Vulnerability in Microsoft Font Driver Could Allow Remote Code Execution (3079904)**
MS15-077	**Vulnerability in ATM Font Driver Could Allow Elevation of Privilege (3077657)**
MS15-076	**Vulnerability in Windows Remote Procedure Call Could Allow Elevation of Privilege (3067505)**
MS15-075	**Vulnerabilities in OLE Could Allow Elevation of Privilege (3072633)**
MS15-074	**Vulnerability in Windows Installer Service Could Allow Elevation of Privilege (3072630)**
MS15-073	**Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3070102)**
MS15-072	**Vulnerability in Windows Graphics Component Could Allow Elevation of Privilege (3069392)**
MS15-071	**Vulnerability in Netlogon Could Allow Elevation of Privilege (3068457)**
MS15-070	**Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3072620)**
MS15-069	**Vulnerabilities in Windows Could Allow Remote Code Execution (3072631)**
MS15-068	**Vulnerabilities in Windows Hyper-V Could Allow Remote Code Execution (3072000)**
MS15-067	**Vulnerability in RDP Could Allow Remote Code Execution (3073094)**
MS15-066	**Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3072604)**
MS15-065	**Security Update for Internet Explorer (3076321)**
MS15-064	**Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3062157)**
MS15-063	**Vulnerability in Windows Kernel Could Allow Elevation of Privilege (3063858)**
MS15-062	**Vulnerability in Active Directory Federation Services Could Allow Elevation of Privilege (3062577)**
MS15-061	**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057839)**
MS15-060	**Vulnerability in Microsoft Common Controls Could Allow Remote Code Execution (3059317)**
MS15-059	**Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3064949)**
MS15-058	**Vulnerabilities in SQL Server Could Allow Remote Code Execution (3065718)**
MS15-057	**Vulnerability in Windows Media Player Could Allow Remote Code Execution (3033890)**
MS15-056	**Cumulative Security Update for Internet Explorer (3058515)**
MS15-055	**Vulnerability in Schannel Could Allow Information Disclosure (3061518)**
MS15-054	**Vulnerability in Microsoft Management Console File Format Could Allow Denial of Service (3051768)**
MS15-053	**Vulnerabilities in JScript and VBScript Scripting Engines Could Allow Security Feature Bypass (3057263)**
MS15-052	**Vulnerability in Windows Kernel Could Allow Security Feature Bypass (3050514)**
MS15-051	**Vulnerabilities in Windows Kernel-Mode Drivers Could Allow Elevation of Privilege (3057191)**

MS15-050	Vulnerability in Service Control Manager Could Allow Elevation of Privilege (3055642)
MS15-049	Vulnerability in Silverlight Could Allow Elevation of Privilege (3058985)
MS15-048	Vulnerabilities in .NET Framework Could Allow Elevation of Privilege (3057134)
MS15-047	Vulnerabilities in Microsoft SharePoint Server Could Allow Remote Code Execution (3058083)
MS15-046	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3057181)
MS15-045	Vulnerability in Windows Journal Could Allow Remote Code Execution (3046002)
MS15-044	Vulnerabilities in Microsoft Font Drivers Could Allow Remote Code Execution (3057110)
MS15-043	Cumulative Security Update for Internet Explorer (3049563)
MS15-042	Vulnerability in Windows Hyper-V Could Allow Denial of Service (3047234)
MS15-041	Vulnerability in .NET Framework Could Allow Information Disclosure (3048010)
MS15-040	Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (3045711)
MS15-039	Vulnerability in XML Core Services Could Allow Security Feature Bypass (3046482)
MS15-038	Vulnerabilities in Microsoft Windows Could Allow Elevation of Privilege (3049576)
MS15-037	Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (3046269)
MS15-036	Vulnerabilities in Microsoft SharePoint Server Could Allow Elevation of Privilege (3052044)
MS15-035	Vulnerability in Microsoft Graphics Component Could Allow Remote Code Execution (3046306)
MS15-034	Vulnerability in HTTP.sys Could Allow Remote Code Execution (3042553)
MS15-033	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3048019)
MS15-032	Cumulative Security Update for Internet Explorer (3038314)
MS15-031	Vulnerability in Schannel Could Allow Security Feature Bypass (3046049)
MS15-030	Vulnerability in Remote Desktop Protocol Could Allow Denial of Service (3039976)
MS15-029	Vulnerability in Windows Photo Decoder Component Could Allow Information Disclosure (3035126)
MS15-028	Vulnerability in Windows Task Scheduler Could Allow Security Feature Bypass (3030377)
MS15-027	Vulnerability in NETLOGON Could Allow Spoofing (3002657)
MS15-026	Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3040856)
MS15-025	Vulnerabilities in Windows Kernel Could Allow Elevation of Privilege (3038680)
MS15-024	Vulnerability in PNG Processing Could Allow Information Disclosure (3035132)
MS15-023	Vulnerabilities in Kernel-Mode Driver Could Allow Elevation of Privilege (3034344)
MS15-022	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3038999)
MS15-021	Vulnerabilities in Adobe Font Driver Could Allow Remote Code Execution (3032323)

MS15-020	**Vulnerabilities in Microsoft Windows Could Allow Remote Code Execution (3041836)**
MS15-019	**Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3040297)**
MS15-018	**Cumulative Security Update for Internet Explorer (3032359)**
MS15-017	**Vulnerability in Virtual Machine Manager Could Allow Elevation of Privilege (3035898)**
MS15-016	**Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3029944)**
MS15-015	**Vulnerability in Microsoft Windows Could Allow Elevation of Privilege (3031432)**
MS15-014	**Vulnerability in Group Policy Could Allow Security Feature Bypass (3004361)**
MS15-013	**Vulnerability in Microsoft Office Could Allow Security Feature Bypass (3033857)**
MS15-012	**Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3032328)**
MS15-011	**Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)**
MS15-010	**Vulnerabilities in Windows Kernel-Mode Driver Could Allow Remote Code Execution (3036220)**
MS15-009	**Security Update for Internet Explorer (3034682)**
MS15-008	**Vulnerability in Windows Kernel-Mode Driver Could Allow Elevation of Privilege (3019215)**
MS15-007	**Vulnerability in Network Policy Server RADIUS Implementation Could Cause Denial of Service (3014029)**
MS15-006	**Vulnerability in Windows Error Reporting Could Allow Security Feature Bypass (3004365)**
MS15-005	**Vulnerability in Network Location Awareness Service Could Allow Security Feature Bypass (3022777)**
MS15-004	**Vulnerability in Windows Components Could Allow Elevation of Privilege (3025421)**
MS15-003	**Vulnerability in Windows User Profile Service Could Allow Elevation of Privilege (3021674)**
MS15-002	**Vulnerability in Windows Telnet Service Could Allow Remote Code Execution (3020393)**
MS15-001	**Vulnerability in Windows Application Compatibility Cache Could Allow Elevation of Privilege (3023266)**

2014- Microsoft® Windows Patches Tested with MAXPRO®NVR

Microsoft KnowledgeBase Article ID	Description
MS14-085	Vulnerability in Microsoft Graphics Component Could Allow Information Disclosure (3013126)
MS14-084	Vulnerability in VBScript Scripting Engine Could Allow Remote Code Execution (3016711)
MS14-083	Vulnerabilities in Microsoft Excel Could Allow Remote Code Execution (3017347)
MS14-082	Vulnerability in Microsoft Office Could Allow Remote Code Execution (3017349)
MS14-081	Vulnerabilities in Microsoft Word and Microsoft Office Web Apps Could Allow Remote Code Execution (3017301)
MS14-080	Cumulative Security Update for Internet Explorer (3008923)
MS14-079	Vulnerability in Kernel Mode Driver Could Allow Denial of Service (3002885)
MS14-078	Vulnerability in IME (Japanese) Could Allow Elevation of Privilege (2992719)
MS14-077	Vulnerability in Active Directory Federation Services Could Allow Information Disclosure (3003381)
MS14-076	Vulnerability in Internet Information Services (IIS) Could Allow Security Feature Bypass (2982998)
MS14-075	Vulnerabilities in Microsoft Exchange Server Could Allow Elevation of Privilege (3009712)
MS14-074	Vulnerability in Remote Desktop Protocol Could Allow Security Feature Bypass (3003743)
MS14-073	Vulnerability in Microsoft SharePoint Foundation Could Allow Elevation of Privilege (3000431)
MS14-072	Vulnerability in .NET Framework Could Allow Elevation of Privilege (3005210)
MS14-071	Vulnerability in Windows Audio Service Could Allow Elevation of Privilege (3005607)
MS14-070	Vulnerability in TCP/IP Could Allow Elevation of Privilege (2989935)
MS14-069	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (3009710)
MS14-068	Vulnerability in Kerberos Could Allow Elevation of Privilege (3011780)
MS14-067	Vulnerability in XML Core Services Could Allow Remote Code Execution (2993958)
MS14-066	Vulnerability in Schannel Could Allow Remote Code Execution (2992611)
MS14-065	Cumulative Security Update for Internet Explorer (3003057)
MS14-064	Vulnerabilities in Windows OLE Could Allow Remote Code Execution (3011443)
MS14-063	Vulnerability in FAT32 Disk Partition Driver Could Allow Elevation of Privilege (2998579)
MS14-062	Vulnerability in Message Queuing Service Could Allow Elevation of Privilege (2993254)
MS14-061	Vulnerability in Microsoft Word and Office Web Apps Could Allow Remote Code Execution (3000434)

Microsoft KnowledgeBase Article ID	Description
MS14-060	**Vulnerability in Windows OLE Could Allow Remote Code Execution (3000869)**
MS14-059	**Vulnerability in ASP.NET MVC Could Allow Security Feature Bypass (2990942)**
MS14-058	**Vulnerability in Kernel-Mode Driver Could Allow Remote Code Execution (3000061)**
MS14-057	**Vulnerabilities in .NET Framework Could Allow Remote Code Execution (3000414)**
MS14-056	**Cumulative Security Update for Internet Explorer (2987107)**
MS14-055	**Vulnerabilities in Microsoft Lync Server Could Allow Denial of Service (2990928)**
MS14-054	**Vulnerability in Windows Task Scheduler Could Allow Elevation of Privilege (2988948)**
MS14-053	**Vulnerability in .NET Framework Could Allow Denial of Service (2990931)**
MS14-052	**Cumulative Security Update for Internet Explorer (2977629)**
KB2862152	Microsoft security advisory: Vulnerability in IPsec could allow security feature bypass
KB2871997	Microsoft Security Advisory: Update to improve credentials protection and management: May 13, 2014
KB2898857	MS14-009: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: February 11, 2014
KB2909210	MS14-011: Description of the security update for Visual Basic Scripting Edition (VBScript) 5.8: February 11, 2014
KB2911501	MS14-009: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: February 11, 2014
KB2922229	Vulnerability in Windows file handling component could allow remote code execution: April 8, 2014
KB2926765	MS14-027: Description of the security update for Windows: May 13, 2014
KB2929733	The first stage of the WER protocol is not SSL encrypted in Windows
KB2931356	MS14-026: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: May 13, 2014
KB2939576	MS14-033: Description of the security update for MSXML: June 10, 2014
KB2957189	MS14-031: Description of the security update for TCP for Windows: June 10, 2014
KB2957503	MS14-036: Description of the security update for Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, and Windows Server 2003: June 10, 2014
KB2957509	MS14-036: Description of the security update for Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, and Windows Server 2003: June 10, 2014
KB2961072	MS14-040: Description of the security update for an ancillary function driver: July 8, 2014
KB2962872	MS14-037: Security update for Internet Explorer versions 6, 7, 8, 9, 10, and 11: July 8, 2014
KB2971850	MS14-038: Description of the security update for Windows: July 8, 2014

Microsoft KnowledgeBase Article ID	Description
KB2972280	MS14-041: Description of the security update for DirectShow: July 8, 2014
KB2973201	MS14-039: Description of the security update for Windows on-screen keyboard: July 8, 2014
KB2973351	Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed: July 8, 2014

2013- Microsoft® Windows Patches Tested with MAXPRO®NVR

Microsoft KnowledgeBase Article ID	Description
KB2798162	Update to improve messaging in dialog boxes when you run executable files in Windows.
KB2813430	Enables administrators to update trusted and disallowed CTLs in disconnected environments in Windows
KB2832414	MS13-052: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: July 9, 2013
KB2836942	Update for the .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1 (June 2013)
KB2836943	Update for the .NET Framework 3.5.1 on Windows 7 SP1 and Windows Server 2008 R2 SP1: September 2013
KB2839894	MS13-050: Vulnerability in Windows print spooler components could allow elevation of privilege: June 11, 2013
KB2840631	MS13-052: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: July 9, 2013
KB2847311	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
KB2847927	MS13-058: Vulnerability in Windows Defender could allow elevation of privilege: July 9, 2013
KB2855844	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
KB2861191	MS13-082: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: October 8, 2013
KB2861855	Microsoft Security Advisory: Updates to improve Remote Desktop Protocol network-level authentication: August 13, 2013
KB2862330	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2862335	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2862966	An update is available that improves management of weak certificate cryptographic algorithms in Windows
KB2862973	Microsoft Security Advisory: Update for deprecation of MD5 hashing algorithm for Microsoft root certificate program: August 13, 2013

Microsoft KnowledgeBase Article ID	Description
KB2864058	MS13-083: Vulnerability in Windows Common Control Library could allow remote code execution: October 8, 2013
KB2864202	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2868038	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2868626	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
KB2876284	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
KB2876331	MS13-089: Vulnerability in Windows Graphics Device Interface could allow remote code execution: November 12, 2013
KB2884256	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2887069	MS13-101: Description of the security update for Windows kernel-mode drivers: December 10, 2013
KB2892074	MS13-099: Description of the security update for Windows Script 5.8: December 10, 2013
KB2893294	MS13-098: Vulnerability in Windows could allow remote code execution: December 10, 2013
KB2900986	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013
KB958488	An update is available for Microsoft .NET Framework 3.5 Service Pack 1 on Windows 7 and Windows Server 2008 R2
KB976902	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available

2016 -Windows 7, 32 Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS

Microsoft KnowledgeBase Article ID	Description
Kb2534111	Computer name cannot contain only numbers" error message when you install Windows 7 by using Windows 7 SP1 integrated installation media
MS15-088	This security update helps resolve an information disclosure vulnerability in Windows, Internet Explorer, and Microsoft Office. To exploit the vulnerability, an attacker would first have to use another vulnerability in Internet Explorer to run code in the sandboxed process. The attacker could then run Notepad, Visio, PowerPoint, Excel, or Word by using an unsafe command-line parameter to effect information disclosure. To be protected from the vulnerability, customers must apply the updates that are provided in this bulletin and also the update for Internet Explorer that is provided in MS15-079. Similarly, customers who are running an affected Office product must also install the applicable updates that are provided in MS15-081.
MS15-090	Vulnerabilities in Windows could allow elevation of privilege.

Microsoft KnowledgeBase Article ID	Description
MS15-085	This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker inserts a malicious USB device into a target system. An attacker could then write a malicious binary to disk and execute the code.
MS15-080	This security update resolves vulnerabilities in the Microsoft .NET Framework and Microsoft Silverlight. These vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
MS15-101	This update resolves vulnerabilities in the Microsoft .NET Framework that could allow elevation of privilege if a user runs a specially crafted .NET Framework application.
MS15-082	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RDP file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs, could view, change, or delete data, or could create new accounts that have full user rights.
MS15-084	This security update resolves vulnerabilities in Microsoft Windows and Microsoft Office. The vulnerabilities could allow information disclosure by either exposing memory addresses if a user clicks a specially crafted link or by explicitly allowing the use of Secure Sockets Layer (SSL) 2.0. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.
MS15-089	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker forces an encrypted Secure Socket Layer (SSL) 2.0 session and uses a man-in-the-middle (MiTM) attack to decrypt parts of the encrypted traffic.
KB3077715	This update supersedes and replaces the update that is described in Microsoft Knowledge Base article 3013410 that was released in December 2014. All additional time zone changes that were released as hotfixes after update 3013410 was released are incorporated in this update.
MS15-080	This security update resolves vulnerabilities in Windows that could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
MS15-109	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.
MS15-121	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow spoofing if an attacker performs a man-in-the-middle (MiTM) attack between a client and a legitimate server.
MS15-102	This security update resolves vulnerabilities in Windows that could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
MS15-097	In addition to the changes that are listed for the vulnerabilities that are described in Microsoft Security Bulletin MS15-097, this security bulletin addresses a defense-in-depth update for the secdrv.sys driver, a third-party driver. The update turns off the service for the secdrv.sys driver. This may affect the ability to run some older games.
MS15-097	This security update resolves vulnerabilities in Windows, Microsoft Office, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded OpenType fonts.
MS15-119	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a computer and runs specially crafted code that exploits the vulnerability.
MS15-109	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.
KB3097966	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
MS15-118	This update resolves vulnerabilities in the Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an attacker injects a client-side script into a user's browser.
MS15-128	This update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
MS15-114	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who have administrative user rights.
MS15-122	This security update resolves a security feature bypass in Windows. An attacker could bypass Kerberos authentication on a computer and decrypt drives that have BitLocker enabled. The bypass can be exploited only if the computer has BitLocker enabled without a PIN or USB key, the computer is domain joined, and the attacker has physical access to the computer.
MS15-117	This security update resolves a vulnerability in Microsoft Windows NDIS. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
MS15-115	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to open a specially crafted document or to go to an untrusted webpage that contains embedded fonts.
MS15-124	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
MS15-132 KB3108381	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
MS16-007 KB3109560 KB3110329	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
MS15-134	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
MS15-130	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains specially crafted fonts.
MS15-128	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application.
MS15-133	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed.
KB3112343	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1.
MS16-013	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
MS16-019	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
KB3123479	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
MS16-005	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if a user visits a malicious website.
MS16-001	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
MS16-016	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker uses the Microsoft Web Distributed Authoring and Versioning (WebDAV) client to send specifically crafted input to a server.
MS16-014 kB3126593	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
MS16-019	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
MS16-035 KB3135988	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
KB3138612	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1.
MS16-027 KB3138962	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
MS16-033	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker with physical access inserts a specially crafted USB device into the system.
MS16-034	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.
MS16-032	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.
MS16-030	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerabilities to execute malicious code. However, an attacker must first convince a user to open a specially crafted file or a program from either a webpage or an email message.
MS16-031	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application.
MS16-026	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to either open a specially crafted document or visit a webpage that contains specially crafted, embedded OpenType fonts.
MS16-039	This security update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
MS16-039	This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
MS16-044	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.

Microsoft KnowledgeBase Article ID	Description
MS16-040	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user clicks a specially crafted link that could allow an attacker to run malicious code remotely to take control of the user's system. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.
MS16-047	An elevation of privilege vulnerability exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols when they accept authentication levels that do not protect these protocols adequately. The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.
KB958488	This article describes an update that consists of Shared Components for Microsoft .NET Framework on Windows 7 and on Windows Server 2008 R2. This update addresses a set of issues of the Microsoft .NET Framework 3.5 Service Pack 1 (SP1).
KB2533552	An update that prevents a "0xc0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available

2016 -Windows 7, 64 Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS

Microsoft KnowledgeBase Article ID	Description
KB2798162	Update to improve messaging in dialog boxes when you run executable files in Windows.
KB2813430	This software update provides the following improvements for Windows: Enables administrators to configure domain-joined computers to use the auto update feature for both trusted and disallowed Certificate Trust Lists (CTLs). The computers can use the auto update feature without accessing the Windows Update site. Enables administrators to configure domain-joined computers to independently select trusted and disallowed CTLs by using the auto update feature. Enables administrators to examine the set of the root certification authorities (CAs) in the Microsoft Root Certificate Program.
KB2836943	An update for the Microsoft .NET Framework 3.5.1 is available. For more information about the issues that the update resolves, see the "Issues that this update resolves" section.
KB2839894	MS13-050: Vulnerability in Windows print spooler components could allow elevation of privilege: June 11, 2013.
KB2862152	Microsoft security advisory: Vulnerability in IPsec could allow security feature bypass
KB2862330	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2862335	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2862973	Microsoft Security Advisory: Update for deprecation of MD5 hashing algorithm for Microsoft root certificate program: August 13, 2013
KB2864202 KB2868038 KB2884256	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2868626	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
KB2871997	Microsoft Security Advisory: Update to improve credentials protection and management: May 13, 2014
KB2887069	MS13-101: Description of the security update for Windows kernel-mode drivers: December 10, 2013
KB2892074	MS13-099: Description of the security update for Windows Script 5.8: December 10, 2013
KB2893294	MS13-098: Vulnerability in Windows could allow remote code execution: December 10, 2013
KB2894844	This security update resolves a vulnerability in the Microsoft .NET Framework 3.5.1 that could allow elevation of privilege on a server system if a user views a specially crafted webpage by using a web browser that can run ASP.NET applications. This security update applies to Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1.
KB2900986	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013

Microsoft KnowledgeBase Article ID	Description
KB2911501	This update resolves vulnerabilities that could allow elevation of privilege if a user goes to a specially crafted website or a website that contains specially crafted web content.
KB2918614	MS14-049: Description of the security update for Windows Installer Service: August 12, 2014
KB2929733	The first stage of the WER protocol is not SSL encrypted in Windows
KB2931356	MS14-026: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: May 13, 2014
KB2937610	MS14-046: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: August 12, 2014
KB2939576	MS14-033: Description of the security update for MSXML: June 10, 2014
KB2957189	MS14-031: Description of the security update for TCP for Windows: June 10, 2014
KB2957509	MS14-036: Description of the security update for Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, and Windows Server 2003: June 10, 2014
KB2961072	MS14-040: Description of the security update for an ancillary function driver: July 8, 2014
KB2968294	MS14-057: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: October 14, 2014
KB2972100	MS14-057: Description of the security update for the .NET Framework 3.5.1 for Windows 7 SP1 and Windows Server 2008 R2 SP1: October 14, 2014
KB2972211	MS14-053: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: September 9, 2014
KB2973201	This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker uses a vulnerability in a low-integrity process to execute the on-screen keyboard (OSK) and upload a specially crafted program to the target system.
KB2973351	Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed: July 8, 2014
KB2976897	MS14-045: Description of the security update for kernel-mode drivers: August 12, 2014
KB2977292	Microsoft security advisory: Update for Microsoft EAP implementation that enables the use of TLS: October 14, 2014
KB2978120	This update resolves a vulnerability in the Microsoft .NET Framework that could allow elevation of privilege.
KB2978668	MS14-047: Vulnerability in LRPC could allow security feature bypass: August 12, 2014
KB2979570	MS14-057: Description of the security update for the .NET Framework 3.5.1 for Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: October 14, 2014
KB2984972	This Remote Desktop Protocol (RDP) 7.1 update enables the Remote Desktop Connection client to perform restricted administration logons. It also enables the Remote Desktop Service that is running on an RD host to perform restricted administration.
KB2990214	This article describes an update that enables you to upgrade your computer from Windows 7 Service Pack 1 (SP1) to a later version of Windows.
KB2991963	MS14-078: Description of the security update for IME: November 11, 2014

Microsoft KnowledgeBase Article ID	Description
KB2992611	MS14-066: Vulnerability in SChannel could allow remote code execution: November 11, 2014
KB2993651	MS14-045: Description of the security update for kernel-mode drivers: August 27, 2014
KB3002657	MS15-027: Vulnerability in NETLOGON could allow spoofing: March 10, 2015
KB3003743	MS14-074: Vulnerability in Remote Desktop Protocol could allow security feature bypass: November 11, 2014
KB3004361	MS15-014: Vulnerability in Group Policy could allow security feature bypass: February 10, 2015
KB3004375	Microsoft is announcing the availability of an update for supported editions of Windows 7, Windows Server 2008R2, Windows 8, and Windows Server 2012. This update expands the Audit Process Creation policy to include the command information that is passed to every process. This is a new feature that provides valuable information to help administrators investigate, monitor, and troubleshoot security-related issues on their networks.
KB3005607	MS14-071: Vulnerability in Windows Audio Service could cause Elevation of Privilege: November 11, 2014
KB3006226	MS14-064: Description of the security update for Windows OLE: November 11, 2014
KB3010788	MS14-064: Description of the security update for Windows OLE: November 11, 2014
KB3011780	MS14-068: Vulnerability in Kerberos could allow elevation of privilege: November 18, 2014
KB3014029	MS15-007: Vulnerability in Network Policy Server RADIUS implementation could cause denial of service: January 13, 2015
KB2992611	MS14-066: Vulnerability in SChannel could allow remote code execution: November 11, 2014
KB3019978	MS15-004: Description of the security update for Windows: January 13, 2015
KB3020369	The servicing stack includes the files and resources that are required to service a Windows image. This includes the Package Manager executable, the required servicing libraries, and other resources. The servicing stack is included in all Windows installations.
KB3021674	MS15-003: Vulnerability in Windows User Profile service could allow elevation of privilege: January 13, 2015
KB3022777	MS15-005: Vulnerability in Network Location Awareness service could allow security feature bypass: January 13, 2015
KB3023215	MS15-048: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: May 12, 2015
KB3030377	MS15-028: Vulnerability in Windows Task Scheduler could allow security feature bypass: March 10, 2015
KB3032323	MS15-021: Vulnerabilities in Adobe font driver could allow remote code execution: March 10, 2015
KB3032655	This update resolves vulnerabilities in the Microsoft .NET Framework. These vulnerabilities could allow denial of service (DoS).
KB3033889	MS15-020: Description of the security update for Windows text services: March 10, 2015

Microsoft KnowledgeBase Article ID	Description
KB3033929	Microsoft security advisory: Availability of SHA-2 code signing support for Windows 7 and Windows Server 2008 R2: March 10, 2015
KB3035126	MS15-029: Vulnerability in Windows Photo Decoder component could allow information disclosure: March 10, 2015
KB3035132	MS15-024: Vulnerability in PNG processing could allow information disclosure: March 10, 2015
KB3037574	MS15-041: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: April 14, 2015
KB3039066	MS15-020: Description of the security update for Windows shell: March 10, 2015
KB3042058	Microsoft security advisory: Update to default cipher suite priority order: May 12, 2015
KB3042553	MS15-034: Vulnerability in HTTP.sys could allow remote code execution: April 14, 2015
KB3045171	MS15-044 and MS15-051: Description of the security update for Windows font drivers
KB3045685	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. To exploit the vulnerabilities, an attacker would first have to log on to the system. This security update addresses the vulnerabilities by correcting how Windows validates impersonation events.
KB3045999	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. To exploit the vulnerabilities, an attacker would first have to log on to the system. This security update addresses the vulnerabilities by correcting how Windows validates impersonation events. For more information about the vulnerabilities, see the "More Information" section.
KB3046017	This security update helps resolve an information disclosure vulnerability in Windows, Internet Explorer, and Microsoft Office. To exploit the vulnerability, an attacker would first have to use another vulnerability in Internet Explorer to run code in the sandboxed process. The attacker could then run Notepad, Visio, PowerPoint, Excel, or Word by using an unsafe command-line parameter to effect information disclosure. To be protected from the vulnerability, customers must apply the updates that are provided in this bulletin and also the update for Internet Explorer that is provided in MS15-079. Similarly, customers who are running an affected Office product must also install the applicable updates that are provided in MS15-081.
KB3046269	This security update resolves a vulnerability in Microsoft Windows. An attacker who successfully exploited the vulnerability could take advantage of a known invalid task to cause Task Scheduler to run a specially crafted application in the context of the System account. An attacker could then do the following: • Install programs • View, change, or delete data • Create new accounts that have full user rights

Microsoft KnowledgeBase Article ID	Description
KB3046306	This security update resolves a vulnerability in Windows that could allow remote code execution if an attacker successfully convinces a user to browse to a specially crafted website, open a specially crafted file, or browse to a working directory that contains a specially crafted Enhanced Metafile (EMF) image file. However, in every case an attacker would have no way to force users to take such actions. An attacker would have to convince users to do this. Typically, the attacker would do this by using enticements in email or instant messaging (IM) messages.
KB3046482	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow security feature bypass if a user clicks a specially crafted link. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.
KB3055642	This security update resolves a vulnerability in Windows Service Control Manager (SCM). This vulnerability is caused when SCM incorrectly verifies impersonation levels. The vulnerability could allow elevation of privilege if an attacker can first log on to the system and then run a specially crafted application that is designed to increase privileges.
KB3057839	This security update resolves vulnerabilities in Windows. The most severe of these vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application. An attacker could then install programs; view, change, or delete data; or create new accounts that have full user rights.
KB3058515	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer. To learn more about the vulnerabilities, see Microsoft Security Bulletin MS15-056. Additionally, this security update includes several non-security-related fixes for Internet Explorer. Check out the deployment information.
KB3059317	This security update resolves a vulnerability in Windows that could allow remote code execution if a user clicks a specially crafted link or a link to specially crafted content and then invokes F12 developer tools in Internet Explorer.
KB3060716	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application or convinces a user to open a specially crafted file that invokes a vulnerable sandboxed application, allowing an attacker to escape the sandbox. This security update is rated Important for all supported releases of Microsoft Windows except Windows 10, which is not affected. For more information, see the Affected Software section.
KB3061518	This security update resolves a vulnerability in Windows. The vulnerability could allow information disclosure when Secure Channel (Schannel) allows the use of a weak Diffie-Hellman ephemeral (DHE) key length of 512 bits in an encrypted Transport Layer Security (TLS) session. Allowing 512-bit DHE keys makes DHE key exchanges weak and vulnerable to various attacks. For an attack to be successful, a server has to support 512-bit DHE key lengths. Windows TLS servers send a default DHE key length of 1,024 bits.
KB3063858	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if a user visits a network share (or visits a website that points to a network share) that contains a specially crafted file. However, in every case an attacker would be unable to force a user to visit such a network share or website.

Microsoft KnowledgeBase Article ID	Description
KB3071756	This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker inserts a malicious USB device into a target system. An attacker could then write a malicious binary to disk and execute the code.
KB3072305	This security update resolves vulnerabilities in the Microsoft .NET Framework and Microsoft Silverlight. These vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
KB3072595	This security update resolves a vulnerability in Active Directory Domain Services (AD DS). The vulnerability could allow denial of service if an authenticated attacker creates multiple computer accounts. To exploit this vulnerability an attacker must have valid credentials.
KB3074543	This update resolves vulnerabilities in the Microsoft .NET Framework that could allow elevation of privilege if a user runs a specially crafted .NET Framework application. To learn more about this vulnerability, see Microsoft Security Bulletin MS15-101.
KB3075220	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RDP file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs, could view, change, or delete data, or could create new accounts that have full user rights.
KB3076895	This security update resolves vulnerabilities in Microsoft Windows and Microsoft Office. The vulnerabilities could allow information disclosure by either exposing memory addresses if a user clicks a specially crafted link or by explicitly allowing the use of Secure Sockets Layer (SSL) 2.0. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.
KB3076949	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker forces an encrypted Secure Socket Layer (SSL) 2.0 session and uses a man-in-the-middle (MiTM) attack to decrypt parts of the encrypted traffic.
KB307771	Microsoft has expanded its online services to a non-proprietary platform with the addition of no-charge Microsoft-sponsored NNTP newsgroups on the Internet. Previously, Microsoft-sponsored electronic service forums were limited to users of CompuServe and MSN. With the creation of these newsgroups, users of Microsoft Access can obtain online service support on the Microsoft Support Web site at http://www.microsoft.com/communities/newsgroups/en-us/default.aspx by using any Internet service provider.
KB3078601	This security update resolves vulnerabilities in Windows that could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
KB3080446	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.

Microsoft KnowledgeBase Article ID	Description
KB3084135	This security update resolves vulnerabilities in Windows that could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
KB3086255	In addition to the changes that are listed for the vulnerabilities that are described in Microsoft Security Bulletin MS15-097, this security bulletin addresses a defense-in-depth update for the secdrv.sys driver, a third-party driver. The update turns off the service for the secdrv.sys driver. This may affect the ability to run some older games.
KB3087039	This security update resolves vulnerabilities in Windows, Microsoft Office, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded OpenType fonts.
KB3092601	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a computer and runs specially crafted code that exploits the vulnerability.
KB3097966	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
KB3097989	This update resolves vulnerabilities in the Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an attacker injects a client-side script into a user's browser.
KB3099862	This update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
KB3101722	This security update resolves a vulnerability in Microsoft Windows NDIS. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
KB3108371	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.
KB3108381	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.
KB3108664	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3108670	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains specially crafted fonts.
KB3109094	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application.
KB3109103	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed.

Microsoft KnowledgeBase Article ID	Description
KB3109560	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3110329	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3112343	This update enables support for additional upgrade scenarios from Windows 7 to Windows 10, and provides a smoother experience when you have to retry an operating system upgrade because of certain failure conditions. This update also improves the ability of Microsoft to monitor the quality of the upgrade experience.
KB3115858	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
KB3122648	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
KB3123479	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
KB3124001	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if a user visits a malicious website.
KB3124275	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
KB3124280	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker uses the Microsoft Web Distributed Authoring and Versioning (WebDAV) client to send specifically crafted input to a server.
KB3126587	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3126593	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3127220	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
KB3133043	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could cause denial of service on a Network Policy Server (NPS) if an attacker sends specially crafted username strings to the NPS. This scenario could prevent RADIUS authentication on the NPS.
KB3134214	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
KB3135983	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
KB3135988	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
KB3138612	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1. This update has a prerequisite.
KB3138910	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
KB3138962	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
KB3139398	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker with physical access inserts a specially crafted USB device into the system.
KB3139852	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.
KB3139914	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.
KB3139940	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerabilities to execute malicious code. However, an attacker must first convince a user to open a specially crafted file or a program from either a webpage or an email message.
KB3140410	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application.
KB3140735	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to either open a specially crafted document or visit a webpage that contains specially crafted, embedded OpenType fonts.
KB3142042	This security update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
KB3145739	This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.

Microsoft KnowledgeBase Article ID	Description
KB3146706	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.
KB3146963	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user clicks a specially crafted link that could allow an attacker to run malicious code remotely to take control of the user's system. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.
KB3149090	An elevation of privilege vulnerability exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols when they accept authentication levels that do not protect these protocols adequately. The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.
KB958488	This article describes an update that consists of Shared Components for Microsoft .NET Framework on Windows 7 and on Windows Server 2008 R2. This update addresses a set of issues of the Microsoft .NET Framework 3.5 Service Pack 1 (SP1).
KB2533552	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available

2016 -Windows 8.1, 64/32 Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS

Microsoft KnowledgeBase Article ID	Description
KB 2883200/KB 2894029	The Windows 8.1 and Windows Server 2012 R2 General Availability update rollup is available. This update rollup package provides a set of reliability, performance, and finishing touch improvements to Windows 8.1 and Windows Server 2012 R2. We recommend that you apply this update rollup as part of your regular maintenance routines.
KB2889543	Text is corrupted when it's typed into a webpage that uses Adobe Flash Player after you install security update 2880289.
KB2894179	Computer stops responding in OOBE Wizard stage in Windows 8.1
KB 3119147	Microsoft has released a security advisory for IT professionals about vulnerabilities in Adobe Flash Player in the following web browsers: • Internet Explorer in Windows 8, Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows 10, and Windows 10 version 1511 • Microsoft Edge in Windows 10 and Windows 10 version 1511
KB 3135782	This security update resolves vulnerabilities in Adobe Flash Player when it is installed on all supported editions of Windows Server 2012, Windows 8.1, Windows Server 2012 R2, Windows RT 8.1, Windows 10, and Windows 10 Version 1511. For more information, see the "Affected Software" section. The update addresses the vulnerabilities in Adobe Flash Player by updating the affected Adobe Flash libraries that are contained in Internet Explorer 10, Internet Explorer 11, and Microsoft Edge.

2016 -Windows 2008, 64Bit - Microsoft® Windows Patches Tested with MAXPRO®VMS

Microsoft KnowledgeBase Article ID	Description
KB2534111	“Computer name cannot contain only numbers" error message when you install Windows 7 by using Windows 7 SP1 integrated installation media
KB2803821	MS13-057: Description of the security update for Windows Media Format Runtime 9 and 9.5 (wmvdmod.dll), and for Windows Media Player 11 and 12: July 9, 2013
KB2832414	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
KB2833946	This update resolves a vulnerability in the Microsoft .NET Framework that could allow remote code execution on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
KB2834886	This update resolves a vulnerability that could allow remote code execution on a client system if a user opens a specially crafted document or visits a specially crafted webpage that embeds TrueType font files.
KB2835364	This update resolves a vulnerability that could allow remote code execution on a client system if a user opens a specially crafted document or visits a specially crafted webpage that embeds TrueType font files.
KB2840631	This update resolves a vulnerability in the Microsoft .NET Framework that could allow elevation of privilege on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
KB2844286	This update resolves a vulnerability in the Microsoft .NET Framework that could allow elevation of privilege on a client system if a user views a specially crafted webpage by using a web browser that can run XAML Browser Applications (XBAPs).
KB2845187	MS13-056: Vulnerability in Microsoft DirectShow could allow remote code execution: July 9, 2013
KB2847311	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
Kb2847927	MS13-058: Vulnerability in Windows Defender could allow elevation of privilege: July 9, 2013
KB2849470	MS13-062: Vulnerability in remote procedure call could allow elevation of privilege: August 13, 2013
KB2855844	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
KB2861191	This update resolves vulnerabilities in the Microsoft .NET Framework that could allow remote code execution if a user goes to a website that contains a specially crafted OpenType font (OTF) file by using a browser that can run XBAP applications.
KB2861698	This update resolves a vulnerability in the Microsoft .NET Framework that could allow for denial of service.
KB2861855	Microsoft Security Advisory: Updates to improve Remote Desktop Protocol network-level authentication: August 13, 2013
KB2862152	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.

Microsoft KnowledgeBase Article ID	Description
KB2862335	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2862966	An update is available that improves management of weak certificate cryptographic algorithms in Windows
KB2863240	This update resolves a vulnerability in the Microsoft .NET Framework that could allow for denial of service.
KB2864058	MS13-083: Vulnerability in Windows Common Control Library could allow remote code execution: October 8, 2013
KB2864202	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2868038	MS13-081: Description of the security update for USB drivers: October 8, 2013
KB2868116	This article describes some updates that improve the content in warning messages that you receive when you try to run local executable files in Windows Server 2008, Windows 7, Windows Server 2008 R2, Windows 8, Windows RT, and Windows Server 2012.
KB2868623	MS13-065: Vulnerability in ICMPv6 could allow denial of service: August 13, 2013
KB2868626	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
KB2868725	Microsoft security advisory: Update for disabling RC4
KB2872339	MS13-077: Vulnerability in Windows Service Control Manager could allow elevation of privilege: September 10, 2013
KB2875783	MS13-093: Vulnerability in Windows ancillary function driver could allow information disclosure: November 12, 2013
KB2876284	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
KB2876331	MS13-089: Vulnerability in Windows Graphics Device Interface could allow remote code execution: November 12, 2013
KB2883150	MS13-081: Description of the security update for kernel-mode drivers: October 8, 2013
KB2888505	MS13-088: Cumulative security update for Internet Explorer: November 12, 2013
KB2900986	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013
KB3046017	This security update helps resolve an information disclosure vulnerability in Windows, Internet Explorer, and Microsoft Office. To exploit the vulnerability, an attacker would first have to use another vulnerability in Internet Explorer to run code in the sandboxed process. The attacker could then run Notepad, Visio, PowerPoint, Excel, or Word by using an unsafe command-line parameter to effect information disclosure. To be protected from the vulnerability, customers must apply the updates that are provided in this bulletin and also the update for Internet Explorer that is provided in MS15-079. Similarly, customers who are running an affected Office product must also install the applicable updates that are provided in MS15-081.
KB3060716	MS15-090: Vulnerabilities in Windows could allow elevation of privilege: August 11, 2015
KB3069114	This security update resolves vulnerabilities in Windows. The more severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted Windows Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.

Microsoft KnowledgeBase Article ID	Description
KB3071756	This security update resolves a vulnerability in Windows that could allow elevation of privilege if an attacker inserts a malicious USB device into a target system. An attacker could then write a malicious binary to disk and execute the code.
KB3072305	This security update resolves vulnerabilities in the Microsoft .NET Framework and Microsoft Silverlight. These vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
KB3074543	MS15-101: Description of the security update for the .NET Framework 3.5.1 on Windows 7 Service Pack 1 and Windows Server 2008 R2 Service Pack 1: September 8, 2015
KB3075220	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker first places a specially crafted dynamic link library (DLL) file in the target user's current working directory and then convinces the user to open an RDP file or to launch a program that is designed to load a trusted DLL file but instead loads the attacker's specially crafted DLL file. An attacker who successfully exploited the vulnerabilities could take complete control of an affected system. An attacker could then install programs, could view, change, or delete data, or could create new accounts that have full user rights.
KB3076895	This security update resolves vulnerabilities in Microsoft Windows and Microsoft Office. The vulnerabilities could allow information disclosure by either exposing memory addresses if a user clicks a specially crafted link or by explicitly allowing the use of Secure Sockets Layer (SSL) 2.0. However, in every case an attacker would have no way to force users to click a specially crafted link. An attacker would have to convince users to click the link, typically by way of an enticement in an email or Instant Messenger message.
KB3076949	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow information disclosure if an attacker forces an encrypted Secure Socket Layer (SSL) 2.0 session and uses a man-in-the-middle (MiTM) attack to decrypt parts of the encrypted traffic.
KB3077715	This update supersedes and replaces the update that is described in Microsoft Knowledge Base article 3013410 that was released in December 2014. All additional time zone changes that were released as hotfixes after update 3013410 was released are incorporated in this update. If you have already deployed update 3013410, read the descriptions of the specific time zone changes that are addressed in this article to determine whether you must deploy this update immediately. If no systems are affected directly, you can schedule deployment at the next available opportunity. We recommend that you deploy the most current Windows cumulative time zone update to guarantee the consistency of the time zone database on all systems.
KB3078601	This security update resolves vulnerabilities in Windows that could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded TrueType or OpenType fonts.
KB3080446	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online.

Microsoft KnowledgeBase Article ID	Description
KB3083710	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1. This update is incompatible with Windows Server Update Services (WSUS) servers without the hardening update 2938066.
KB3084135	This security update resolves vulnerabilities in Windows that could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.
KB3086255	MS15-097: Description of the security update for the graphics component in Windows: September 8, 2015
KB3087039	This security update resolves vulnerabilities in Windows, Microsoft Office, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or goes to an untrusted webpage that contains embedded OpenType fonts.
KB3087918	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploits this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less affected than those who operate with administrative user rights.
KB3088195	This security update resolves vulnerabilities in Windows. The more severe of the vulnerabilities could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application. Note Customers who are using local and remote reporting attestation solutions should review the details of CVE-2015-2552. This is discussed in the Microsoft security bulletin that is mentioned in the following paragraph.
KB3092601	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a computer and runs specially crafted code that exploits the vulnerability.
KB3093513	This security update resolves vulnerabilities in Windows. These vulnerabilities could allow remote code execution if a user opens a specially crafted toolbar object in Windows or if an attacker convinces a user to view specially crafted content online
KB3093983	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
KB3097966	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.
KB3097989	This update resolves vulnerabilities in the Microsoft .NET Framework. The most severe of these vulnerabilities could allow elevation of privilege if an attacker injects a client-side script into a user's browser.
KB3099862	This update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
KB3101722	This security update resolves a vulnerability in Microsoft Windows NDIS. The vulnerability could allow elevation of privilege if an attacker logs on to a system and runs a specially crafted application.

Microsoft KnowledgeBase Article ID	Description
KB3108371	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.
KB3108381	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if an attacker accesses a local system and runs a specially crafted application.
KB3108664	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3108669	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if Windows Media Center opens a specially crafted Media Center link (.mcl) file that references malicious code. An attacker who successfully exploited this vulnerability could gain the same user rights as the current user. Customers whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.
KB3108670	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted document or visits an untrusted webpage that contains specially crafted fonts.
KB3109094	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application.
KB3109103	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to a targeted system and runs a specially crafted application that, by way of a race condition, results in references to memory locations that have already been freed.
KB3109560	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3110329	This security update resolves vulnerabilities in Microsoft Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3112343	This update enables support for additional upgrade scenarios from Windows 7 to Windows 10, and provides a smoother experience when you have to retry an operating system upgrade because of certain failure conditions. This update also improves the ability of Microsoft to monitor the quality of the upgrade experience.
KB3115858	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user opens a specially crafted Journal file. Users whose accounts are configured to have fewer user rights on the system could be less affected than users who operate with administrative user rights.
KB3122648	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
KB3123479	Microsoft has released a Microsoft security advisory about this issue for IT professionals. The security advisory contains additional security-related information.

Microsoft KnowledgeBase Article ID	Description
KB3124275	This security update resolves several reported vulnerabilities in Internet Explorer. The most severe of these vulnerabilities could allow remote code execution if a user views a specially crafted webpage in Internet Explorer.
KB3124280	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker uses the Microsoft Web Distributed Authoring and Versioning (WebDAV) client to send specifically crafted input to a server.
KB3126587	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3126593	This security update resolves vulnerabilities in Windows. The most severe of the vulnerabilities could allow remote code execution if an attacker is able to log on to a target system and run a specially crafted application.
KB3127220	This update resolves a vulnerability in the Microsoft .NET Framework. The vulnerability could allow denial of service if an attacker inserts specially crafted XSLT into a client-side XML web part that causes recursive calls on the server.
KB3134214	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker logs on to an affected system and runs a specially crafted application.
KB3135983	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
KB3135988	This update resolves a vulnerability in the Microsoft .NET Framework. The security feature bypass exists in a .NET Framework component that does not properly validate certain elements of a signed XML document.
KB3138612	This article describes an update that contains some improvements to Windows Update Client in Windows 7 Service Pack 1 (SP1) and Windows Server 2008 R2 SP1.
KB3138910	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
KB3138962	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if a user opens specially crafted media content that is hosted on a website.
KB3139398	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker with physical access inserts a specially crafted USB device into the system.
KB3139852	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow elevation of privilege if an attacker logs on to the system and runs a specially crafted application.
KB3139914	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if the Windows Secondary Logon Service fails to properly manage request handles in memory.

Microsoft KnowledgeBase Article ID	Description
KB3139940	This security update resolves vulnerabilities in Microsoft Windows. The vulnerabilities could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerabilities to execute malicious code. However, an attacker must first convince a user to open a specially crafted file or a program from either a webpage or an email message.
KB3140410	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow elevation of privilege if an attacker is able to log on to a target system and run a specially crafted application.
KB3140735	This security update resolves vulnerabilities in Microsoft Windows. The more severe of the vulnerabilities could allow remote code execution if an attacker convinces a user to either open a specially crafted document or visit a webpage that contains specially crafted, embedded OpenType fonts.
KB3142042	This security update resolves vulnerabilities in the Microsoft .NET Framework. The vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
KB3145739	This security update resolves vulnerabilities in Microsoft Windows, Microsoft .NET Framework, Microsoft Office, Skype for Business, and Microsoft Lync. The most severe of the vulnerabilities could allow remote code execution if a user opens a specially crafted document or visits a webpage that contains specially crafted embedded fonts.
KB3146706	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if Windows OLE fails to properly validate user input. An attacker could exploit the vulnerability to execute malicious code. However, an attacker must first convince a user to open either a specially crafted file or a program from either a webpage or an email message.
KB3146963	This security update resolves a vulnerability in Microsoft Windows. The vulnerability could allow remote code execution if a user clicks a specially crafted link that could allow an attacker to run malicious code remotely to take control of the user's system. However, in all cases an attacker would have no way to force a user to click a specially crafted link. An attacker would have to convince a user to click the link, typically by way of an enticement in an email or Instant Messenger message.
KB3149090	An elevation of privilege vulnerability exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) remote protocols when they accept authentication levels that do not protect these protocols adequately. The vulnerability is caused by the way the SAM and LSAD remote protocols establish the Remote Procedure Call (RPC) channel. An attacker who successfully exploited this vulnerability could gain access to the SAM database.
KB958488	This article describes an update that consists of Shared Components for Microsoft .NET Framework on Windows 7 and on Windows Server 2008 R2. This update addresses a set of issues of the Microsoft .NET Framework 3.5 Service Pack 1 (SP1).
KB2533552	An update that prevents a "0xC0000034" error message when you try to install Windows 7 SP1, Windows Server 2008 R2 SP1, or Windows Embedded Standard 7 SP1 is available

2016 -Windows 2012 Server R2 - Microsoft® Windows Patches Tested with MAXPRO®VMS

Microsoft KnowledgeBase Article ID	Description
KB2843630	Update helps unmanaged Office 2010 users work with Microsoft RMS in Windows
KB2862152	Microsoft security advisory: Vulnerability in IPsec could allow security feature bypass
KB2868626	MS13-095: Vulnerability in XML digital signatures could allow denial of service: November 12, 2013
KB2876331	MS13-089: Vulnerability in Windows Graphics Device Interface could allow remote code execution: November 12, 2013
KB2883200	Windows 8.1 and Windows Server 2012 R2 General Availability Update Rollup
KB2884101	MS13-080: Description of the security update for Internet Explorer 11 in Windows 8.1 and Windows Server 2012 R2: October 8, 2013
KB2884846	Windows 8.1 and Windows Server 2012 R2 update rollup: October 2013
KB2887595	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: November 2013
KB2892074	MS13-099: Description of the security update for Windows Script 5.8: December 10, 2013
KB2893294	MS13-098: Vulnerability in Windows could allow remote code execution: December 10, 2013
KB2883200	Windows 8.1 and Windows Server 2012 R2 General Availability Update Rollup
KB2894179	Computer stops responding in OOBE Wizard stage in Windows 8.1
KB2887595	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: November 2013
KB2884846	Windows 8.1 and Windows Server 2012 R2 update rollup: October 2013
KB2898871	This update resolves vulnerabilities that could allow elevation of privilege if a user visits a specially crafted website or a website that contains specially crafted web content.
KB2900986	MS13-090: Cumulative security update for ActiveX Kill Bits: November 12, 2013
KB2901128	This update resolves vulnerabilities which could allow elevation of privilege if a user visits a specially crafted website or a website that contains specially crafted web content.
KB2903939	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: December 2013
KB2904266	December 2013 cumulative time zone update for Windows operating systems
KB2906956	"0x80240017" error when you try to install a Windows Store app in Windows RT 8.1, Windows 8.1, or Windows Server 2012 R2
KB2911106	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: January 2014
KB2912390	MS14-007: Vulnerability in Direct2D could allow remote code execution: February 11, 2014
KB2913152	Windows Photo Viewer prints white lines when you use an XPS driver to print photos in Windows
KB2913270	Windows 8.1 Store improvements: January 2014
KB2913760	Drivers and firmware cannot be updated on Windows 8.1-based devices

Microsoft KnowledgeBase Article ID	Description
KB2916036	MS14-005: Vulnerability in Microsoft XML Core Services could allow information disclosure: February 11, 2014
KB2917929	Compatibility update is available for Windows RT 8.1, Windows 8.1 and Windows Server 2012 R2: February 2014
KB2917993	Screen turns black when it rotates from portrait orientation to landscape orientation in Windows
KB2919355	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update: April 2014
KB2919394	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: February 2014
KB2922229	MS14-019: Vulnerability in Windows file handling component could allow remote code execution: April 8, 2014
KB2923300	You can access only the Start screen after you press the "Windows logo key+Period (.)" keyboard shortcut three times in Windows 8.1
KB2923528	Application cannot be started after upgrading to Windows 8.1
KB2923768	Update improves OneDrive (formerly SkyDrive) experience in Windows RT 8.1 and Windows 8.1
KB2928193	RRAS BPA rules update for Windows Server 2012 R2
KB2928680	Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2 update rollup: March 2014
KB2930275	MS14-015: Vulnerabilities in Windows kernel mode driver could allow elevation of privilege: March 11, 2014
KB2931366	MS14-026: Description of the security update for the .NET Framework 4.5.1 on Windows 8.1, Windows RT 8.1 and Windows Server 2012 R2 for systems that have update 2919355 installed: May 13, 2014
KB2934520	The Microsoft .NET Framework 4.5.2 for Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2
KB2938066	An update to harden Windows Server Update Services
KB2939087	Fix Windows Update errors
KB2954879	Description of the update for .NET Native in Windows 8.1, Windows RT 8.1, and Windows Server 2012 R2
KB2957189	MS14-031: Description of the security update for TCP for Windows: June 10, 2014
KB2961908	Description of the update rollup of revoked noncompliant UEFI modules for systems that do not have the 2919355 update installed: May 13, 2014
KB2962123	MS14-027: Description of the security update for Windows systems that do not have update 2919355 installed: May 13, 2014
KB2967917	July 2014 update rollup for Windows RT 8.1, Windows 8.1, and Windows Server 2012 R2
KB2973201	MS14-039: Description of the security update for Windows on-screen keyboard: July 8, 2014
KB2973351	Microsoft Security Advisory: Registry update to improve credentials protection and management for Windows-based systems that have the 2919355 update installed: July 8, 2014

Microsoft KnowledgeBase Article ID	Description
KB2975061	May 2014 servicing stack update for Windows 8.1 and Windows Server 2012 R2
KB2976897	MS14-045: Description of the security update for kernel-mode drivers: August 12, 2014
KB2977292	Microsoft security advisory: Update for Microsoft EAP implementation that enables the use of TLS: October 14, 2014
KB2989930	"Not Connected" status for a paired Surface Pen in Bluetooth settings on Surface Pro 3
KB2992611	MS14-066: Vulnerability in SChannel could allow remote code execution: November 11, 2014
KB2993651	MS14-045: Description of the security update for kernel-mode drivers: August 27, 2014

Contact Information

Honeywell Security and Fire Products Americas
2700 Blankenbaker Pkwy, Suite 150
Louisville, KY 40299, USA
www.honeywellvideo.com
☏ +1.800.323.4576

Honeywell Security and Fire Europe/South Africa
Aston Fields Road, Whitehouse Industrial Estate
Runcorn, WA7 3DL, United Kingdom
www.honeywell.com/security/uk
☏ +44.01928.754028

Honeywell Security and Fire Caribbean/Latin America
9315 NW 112th Ave.
Miami, FL 33178, USA
www.honeywellvideo.com
☏ +1.305.805.8188

Honeywell Security and Fire Pacific
Level 3, 2 Richardson Place
North Ryde, NSW 2113, Australia
www.honeywellsecurity.com.au
☏ +61.2.9353.7000

Honeywell Security and Fire Asia
35F Tower A, City Center, 100 Zun Yi Road
Shanghai 200051, China
www.asia.security.honeywell.com
☏ +86 21.5257.4568

Honeywell Security and Firey Middle East/N. Africa
Post Office Box 18530
LOB Building 08, Office 199
Jebel Ali, Dubai, United Arab Emirates
www.honeywell.com/security/me
☏ +971.04.881.5506

Honeywell Security and Fire Northern Europe
Ampèrestraat 41
1446 TR Purmerend, The Netherlands
www.honeywell.com/security/nl
☏ +31.299.410.200

Honeywell Security and Fire Deutschland
Johannes-Mauthe-Straße 14
D-72458 Albstadt, Germany
www.honeywell.com/security/de
☏ +49 74 31 / 8 01-18 70

Honeywell Security and Fire France
Immeuble Lavoisier
Parc de Haute Technologie
3-7 rue Georges Besse
92160 Antony, France
www.honeywell.com/security/fr
☏ +33.(0).1.40.96.20.50

Honeywell Security and Fire Group Italia SpA
Via della Resistenza 53/59
20090 Buccinasco
Milan, Italy
www.honeywell.com/security/it
☏ +39.02.4888.051

Honeywell Security and Fire Group España
Avenida de Italia, n° 7, 2a planta
C.T.C. Coslada
28821 Coslada, Madrid, Spain
www.honeywell.com/security/es
☏ +34.902.667.800

Honeywell Security & Fire Pacific
Unit 5, 24-28 River Rd West,
Parramatta NSW - 2150, Australia
www.honeywellsecurity.com.au
HSFPAC.Support@honeywell.com
Ph: 1800 220 345

Honeywell

THE POWER OF **CONNECTED**

www.honeywellvideo.com
+1 800 323 4576 (North America only)
https//honeywellsystems.com/ss/techsupp/index.html

www.honeywell.com/security/uk
+44 (0) 1928 754 028 (Europe only)
https//honeywellsystems.com/ss/techsupp/index.html

Document 800-19154V5 - Rev- C –10/2017