Honeywell

Security Notification
SN 2020-02-04 01

04 February 2020

NWS-3 Authentication Bypass & Directory Traversal Attack

This article contains:

- Summary
- Potential Vulnerability Synopsis
- Affected Products
- Resolution Description
- Appendix: About CVSS

It applies to:

NWS-3 products listed in the "Affected Products and Versions" section of this notice

To mitigate the risk:

- Follow Resolution Description procedure.

Skills prerequisite:

Ability to write attack scripts

Understand HTTP

Summary

This security notification informs users of Honeywell Web Server of a potential software vulnerability that has been identified. Honeywell recommends that immediate steps be taken to ensure this potential vulnerability is mitigated in any installed and operational system.

Attention: Due to the wide variety of security controls, implementations and interfaces, it is the responsibility of each customer to assess the potential impact within a specific operating environment.

Vulnerability Synopsis

1. The Honeywell Fire Web Server's authentication may be bypassed by a capture-replay attack from a web browser.

   CVSS Base Score: 9.3 (Critical)

   Temporal Score: 9.3 (High)

   CVSS Vector
   https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:L/A:N.

2. A potential flaw exists where users may bypass access to restricted location to read files and directories on the webserver.

   CVSS Base Score: 9.4 (Critical)

   Temporal Score: 9.3 (High)

   CVSS Vector
   https://www.first.org/cvss/calculator/3.0#CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:F/RL:O/RC:C.

Affected Products

The potential vulnerability affects the following product versions:

- Notifier Web Server (NWS) Version 3.50 and earlier

Mitigating Factors

Honeywell recommends that customers with potentially affected products should take the following steps to protect themselves:

- Update firmware of **NWS-3** as per the security notification
- Isolate their system from the Internet or create additional layers of defense to their system from the Internet by placing the affected hardware behind a firewall or into a DMZ
- If remote connections to the network are required, consider using a VPN or other means to ensure secure remote connections into the network where the device is located
- Always use strong passwords on installations to prevent unauthorized access

Resolution Description

Honeywell has released a firmware update for all affected products listed above.

The package can be downloaded from: **Here**

Attention: This update should be installed by qualified personnel. Access credentials are required to access this site.

Contacting Support

For help installing, operating, maintaining, and troubleshooting this product, refer to this document and the Webserver installation guide. If you still have questions, contact Technical Support during business hours.

Credit

Thanks to Gjoko Krstikj for reporting this potential vulnerability.

Appendix: About CVSS

The Common Vulnerability Scoring System (CVSS) is an open standard for communicating the characteristics and severity of software vulnerabilities. The Base score represents the intrinsic qualities of a vulnerability. The Temporal score reflects the characteristics of a vulnerability that change over time. The Environmental score is an additional score that can be used by CVSS, but is not supplied as it will differ for each customer.

The Base score has a value ranging from 0 to 10. The Temporal score has the same range and is a modification of the Base score due to current temporary factors.

The severity of the score can be summarized as follows:

Severity Rating	CVSS Score
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

A CVSS score is also represented as a vector string, a compressed textual representation of the values used to derive the score.

Detailed information about CVSS can be found at http://www.first.org/cvss.

DISCLAIMERS

- CUSTOMERS ARE RESPONSIBLE FOR ASSESSING THE IMPACT OF ANY ACTUAL OR POTENTIAL SECURITY VULNERABILITY.
- YOUR USE OF THE INFORMATION ON THIS DOCUMENT OR MATERIALS LINKED FROM THIS DOCUMENT IS AT YOUR OWN RISK.
- HONEYWELL RESERVES THE RIGHT TO CHANGE OR UPDATE THIS DOCUMENT AT ANY TIME AND WITHOUT NOTICE.
- HONEYWELL PROVIDES THE CVSS SCORES “AS IS” WITHOUT WARRANTY OF ANY KIND. HONEYWELL DISCLAIMS THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PURPOSE AND MAKES NO EXPRESS WARRANTIES EXCEPT AS MAY BE STATED IN A WRITTEN AGREEMENT WITH AND FOR ITS CUSTOMERS
- IN NO EVENT WILL HONEYWELL BE LIABLE TO ANYONE FOR ANY DIRECT, INDIRECT, SPECIAL, OR CONSEQUENTIAL DAMAGES.