Product Security Bulletin

Honeywell

Apache log4j Vulnerability

Security Bulletin #: 2021-SPS-12-14-01-V2

Publish Date: 12-16-2021

CVSS v3.0 Base Score: 10

Reference: CVE-2021-44228, CVE-2021-45046, CVE-2021-45105

Summary

Honeywell is actively addressing the log4j Remote Code Execution (RCE) and Distributed Denial of Service (DDOS) vulnerabilities recently disclosed as CVE-2021-44228, CVE-2021-45046 and CVE-2021-45105.

Honeywell Productivity Solutions and Services, part of Honeywell Safety and Productivity Solutions, are actively updating affected products and are making those updates available to our customers via normal product support channels. As of the date of this bulletin, only certain Voice applications have been identified as impacted.

For information on specific updates for your products, log into the tech support portal: https://honeywell.custhelp.com/app/answers/detail/a_id/3109

If you have questions about other products, please reach out to your normal product support channel.

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.

Mitigating Factors

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

- Update software and firmware of vulnerable products as updates become available;
- For existing products/versions that are vulnerable, where possible configure the Java Virtual Machine (JVM) flags, classpaths, and/or environment variables as called out in the CVE to disable the vulnerable feature in log4j;
- 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; and
- 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.

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.