Product Security Advisory

Apache Log4j (CVE-2021-44228)

TLP:WHITE

No restriction on distribution

HID-PSA-2021-04v3

2021-December-17

Severity: CRITICAL

Overview:

A vulnerability in Apache Log4j, has been identified and is known to be under active exploitation. This vulnerability allows arbitrary code execution over a remote connection. It is very easy exploit and has been given the highest severity rating.

Affected Products

Authentication Appliance versions 8.3 to 8.5

Authentication Server versions 8.3 to 8.5

Unaffected Products

See HID Global Product Security Advisory HID-PSA-2021-03 for a list of products unaffected by this vulnerability.

Impact

If an attacker can send messages, even unauthenticated, to these products, they may be able to exploit the vulnerability and execute malicious code on the devices.

Mitigation

Note: Based on new information, HID Global has learned that the mitigation provided in the original HID-PSA-2021-04 Product Security Advisory will not be effective. Only patching the vulnerable software mitigates this vulnerability. See Next Steps for information about Hot Fixes.

Next Steps:

HID Global engineering teams are developing additional mitigations to address this issue permanently.

A Hot Fix for the following versions are now available through the HID® ActivID® Customer Portal (https://iamsportal.hidglobal.com/products):

- Authentication Appliance 8.4
- Authentication Appliance 8.5
- Authentication Server 8.4
- Authentication Server 8.5

The following products have limited sustaining support. If you are using these products, please contact your HID representative for next steps.

- Authentication Appliance 8.3
- Authentication Server 8.3

Contact Information:

If you have additional questions, please contact your HID representative.

If you suspect that an HID Global product has been the target of an attack, please contact HID Technical Support at https://www.hidglobal.com/support.

References:

Apache's Disclosure: https://logging.apache.org/log4j/2.x/security.html

Red Hat JBoss: https://access.redhat.com/security/vulnerabilities/RHSB-2021-009

IBM WebSphere: https://www.ibm.com/blogs/psirt/security-bulletin-vulnerability-in-apache-log4j-affects-websphere-application-server-cve-2021-44228/