Corero Network Security

Advisory of Corero Impact from Log4j2 Vulnerability

Advisory ID: 12102021-3
Published: 20 December 2021
CVEs: CVE-2021-44228 / CVE-2021-45046 / CVE-2021-45105 - Apache Log4j2 (Log4Shell / LogJam)

Summary

A critical vulnerability (CVE-2021-44228) in the Apache Log4j2 Java-based logging utility was made public on Friday 10th December 2021, followed to two further vulnerabilities (CVE-2021-45046/45105), of much lower risk, over the following days. For products containing the Log4j2 utility, the initial vulnerability enables an attacker, who is able to control log messages or log message parameters, to execute arbitrary code loaded from LDAP a server, when message lookup substitution is enabled.

Corero has undertaken a complete and thorough analysis of all software components of our SmartWall DDoS protection solutions to determine any exposure to these vulnerabilities.

SmartWall Status

The following Corero products are NOT impacted by CVE-2021-44228/45046/45105:

- SmartWall Service Portal (SSP) – all versions
- SmartWall SecureWatch Analytics (SWA) – all versions
- SmartWall Central Management Server (CMS) – versions prior to 10.0.0
- SmartWall Network Threat Defense (NTD) appliances – NTD280, NTD1100, vNTD – all versions
- SmartWall Network Bypass Appliances (NBA) – all versions

The following Corero SmartWall products and versions ARE impacted by CVE-2021-44228/45046:

- SmartWall Threat Defense System CMS versions 10.0.0-10.2.2 and 11.0.0/11.0.1
- SmartWall Threat Defense Director CMS versions 10.3.0-10.3.2

CMS versions, without the Log4j2 library components that are vulnerable to CVE-2021-44228/45046, have been made available as follows:

- SmartWall Threat Defense System CMS version 10.2.3
- SmartWall Threat Defense System CMS version 11.2.0
- SmartWall Threat Defense Director CMS version 10.3.3

Corero has also now assessed the most recently disclosed vulnerability (CVE-2021-45105) against these latest updated CMS versions and determined that the SmartWall implementation is not susceptible.

Recommended Action:

All SmartWall deployments should be upgraded as soon as possible to prevent exposure to this critical vulnerability in the Apache Log4j2 component.

- All SmartWall Threat Defense Systems running 10.2.2, or earlier, should upgrade CMS to 10.2.3 or 11.2.0
- All SmartWall Threat Defense Systems running 11.0.0/11.0.1 should upgrade CMS to 11.2.0
- All SmartWall Threat Defense Director deployments should upgrade CMS to 10.3.3

Please contact your Corero support representative for more information.