Corero Network Security

Advisory of Corero Impact from Spring4Shell Vulnerability

Advisory ID: 04042022-1
Published: 4 April 2022
CVEs: CVE-2022-22965 - Spring vulnerability (Spring4Shell)

Summary

A critical vulnerability (CVE-2022-22965) in the Spring framework for Java was made public on Friday 1st April 2022. For affected products, the vulnerability could allow an attacker to execute arbitrary code loaded into the affected product.

Corero has undertaken an 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-2022-22965:

- SmartWall Service Portal (SSP) – all versions
- SmartWall SecureWatch Analytics (SWA) – all versions
- SmartWall Network Threat Defense (NTD) appliances– all versions
- SmartWall Network Bypass Appliances (NBA) – all versions

The following Corero SmartWall products and versions may be impacted by CVE-2022-22965:

- SmartWall Threat Defense System CMS versions 10.0.0-10.2.3 and 11.0.0-11.2.2
- SmartWall Threat Defense Director CMS versions 10.3.0-10.3.3

Based on available information, Corero has NOT been able to successfully exploit this vulnerability against any currently supported SmartWall CMS version.

CMS versions that mitigate this vulnerability are being made available as follows:

- SmartWall Threat Defense System CMS version 10.2.4
- SmartWall Threat Defense System CMS version 11.2.3
- SmartWall Threat Defense Director CMS version 10.3.4

Recommended Action:

All SmartWall deployments should be upgraded as soon as possible to prevent exposure to this critical Spring framework vulnerability.

- All SmartWall Threat Defense Systems running 10.x.x, or earlier, should upgrade CMS to 10.2.4 or 11.2.3
- All SmartWall Threat Defense Systems running 11.x.x should upgrade CMS to 11.2.3
- All SmartWall Threat Defense Director deployments should upgrade CMS to 10.3.4

Please contact your Corero support representative for more information.