SSA-254054: Spring Framework Vulnerability (Spring4Shell or SpringShell, CVE-2022-22965) - Impact to Siemens Products

Publication Date: 2022-04-19
Last Update: 2022-10-11
Current Version: V1.3
CVSS v3.1 Base Score: 9.8

SUMMARY

A vulnerability in Spring Framework was disclosed, that could allow remote unauthenticated attackers to execute code on vulnerable systems. The vulnerability is tracked as CVE-2022-22965 and is also known as “Spring4Shell” or “SpringShell”.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Operation Scheduler: All versions < 2.0.4	Update to V2.0.4 or later version See further recommendations from section Workarounds and Mitigations
SIMATIC Speech Assistant for Machines (SAM): All versions < V1.2.1	Update to V1.2.1 or later version. Please contact customer support to obtain the patch See further recommendations from section Workarounds and Mitigations
SINEC NMS: All versions < V1.0.3	Update to V1.0.3 or later version https://support.industry.siemens.com/cs/ww/en/view/109813788/ See further recommendations from section Workarounds and Mitigations
SiPass integrated V2.80: All versions	Apply the patch https://support.industry.siemens.com/cs/ww/en/view/109805711/ See further recommendations from section Workarounds and Mitigations
SiPass integrated V2.85: All versions	Apply the patch https://support.industry.siemens.com/cs/ww/en/view/109805711/ See further recommendations from section Workarounds and Mitigations
Siveillance Identity V1.5: All versions	Update to V1.5 SP4 and apply the patch https://support.industry.siemens.com/cs/ww/en/view/109810454/ See further recommendations from section Workarounds and Mitigations
Siveillance Identity V1.6: All versions	Update to V1.6 SP1 and apply the patch https://support.industry.siemens.com/cs/ww/en/view/109810454/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Block both incoming and outgoing connections between the system and the Internet

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

Operation Scheduler is a tool that enables security operators to intelligently perform routine tasks. It can be used to schedule maintenance tasks.

SINEC NMS is a new generation of the Network Management System (NMS) for the Digital Enterprise. This system can be used to centrally monitor, manage, and configure networks.

SiPass integrated is a powerful and extremely flexible access control system.

Siveillance Identity is an intuitive web-based self-service portal that offers in-house access request management across multiple sites.

SIMATIC Speech Assistant for Machines (SAM) is a voice assistant that allows users to communicate directly with their machines through verbal communication.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.1 (CVSS v3.1) (https://www.first.org/cvss/). The CVSS environmental score is specific to the customer's environment and will impact the overall CVSS score. The environmental score should therefore be individually defined by the customer to accomplish final scoring.

An additional classification has been performed using the CWE classification, a community-developed list of common software security weaknesses. This serves as a common language and as a baseline for weakness identification, mitigation, and prevention efforts. A detailed list of CWE classes can be found at: https://cwe.mitre.org/.

Vulnerability CVE-2022-22965

A Spring MVC or Spring WebFlux application running on JDK 9+ may be vulnerable to remote code execution (RCE) via data binding. The specific exploit requires the application to run on Tomcat as a WAR deployment. If the application is deployed as a Spring Boot executable jar, i.e. the default, it is not vulnerable to the exploit. However, the nature of the vulnerability is more general, and there may be other ways to exploit it.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

For further inquiries on security vulnerabilities in Siemens products and solutions, please contact the Siemens ProductCERT:

https://www.siemens.com/cert/advisories

HISTORY DATA

V1.0 (2022-04-19): Publication Date
V1.1 (2022-04-27): Added solution for Siveillance Identity
V1.2 (2022-06-14): Added affected products SIMATIC Speech Assistant for Machines (SAM) and SINEC NMS
V1.3 (2022-10-11): Added fix for SINEC NMS

TERMS OF USE