

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

Publication Date: 2022-04-19
 Last Update: 2022-04-27
 Current Version: V1.1
 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 is currently investigating to determine which products are affected and is continuously updating this advisory as more information becomes available.

Siemens has released updates for several affected products and recommends to update to the latest versions. Siemens is preparing further updates and recommends specific countermeasures for products where updates are not, or not yet available.

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
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:

- If, for a particular product listed in the table above, no remediation or specific mitigation is given: 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.

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.

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

TERMS OF USE

Siemens Security Advisories are subject to the terms and conditions contained in Siemens' underlying license terms or other applicable agreements previously agreed to with Siemens (hereinafter "License Terms"). To the extent applicable to information, software or documentation made available in or through a Siemens Security Advisory, the Terms of Use of Siemens' Global Website (https://www.siemens.com/terms_of_use, hereinafter "Terms of Use"), in particular Sections 8-10 of the Terms of Use, shall apply additionally. In case of conflicts, the License Terms shall prevail over the Terms of Use.