# SSA-501673: Apache Log4j Denial of Service Vulnerability (CVE-2021-45105) - Impact to Siemens Products

| | |
|---|---|
| Publication Date: | 2021-12-19 |
| Last Update: | 2021-12-19 |
| Current Version: | V1.0 |
| CVSS v3.1 Base Score: | 7.5 |

## SUMMARY

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 contain a vulnerability (CVE-2021-45105) that could allow attackers to cause a denial of service condition in affected applications [1].

This advisory informs about the impact of CVE-2021-45105 to Siemens products and the corresponding remediation and mitigation measures. The vulnerability is different from the JNDI lookup vulnerabilities, the impact of which is documented in SSA-661247 [2].

Currently, no products vulnerable to CVE-2021-45105 have been identified.

Siemens is investigating to determine which products are affected and is continuously updating this advisory as more information becomes available. See section Additional Information for more details regarding the investigation status.

[1] https://logging.apache.org/log4j/2.x/security.html

[2] https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| No product currently identified as affected:<br>No versions | The table will be updated in case vulnerable products become known. |

## WORKAROUNDS AND MITIGATIONS

Siemens has not identified any additional specific workarounds or mitigations. Please follow the General Security Recommendations.

Product specific mitigations can be found in the section Affected Products and Solution.

## 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

## 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-2021-45105

Apache Log4j2 versions 2.0-alpha1 through 2.16.0 did not protect from uncontrolled recursion from self-referential lookups, when the logging configuration uses a non-default Pattern Layout with a Context Lookup (for example, $${ctx:loginId}).

This could allow attackers with control over Thread Context Map (MDC) input data to craft malicious input data that contains a recursive lookup, resulting in a denial of service condition.

| | |
|---|---|
| CVSS v3.1 Base Score | 7.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C |
| CWE | CWE-674: Uncontrolled Recursion |

## ADDITIONAL INFORMATION

For more information on CVE-2021-45105 refer to:

- Apache Log4j security site: https://logging.apache.org/log4j/2.x/security.html
- US NVD Vulnerability entry: https://nvd.nist.gov/vuln/detail/CVE-2021-45105

The impact of other Apache log4j vulnerabilities to Siemens products is described in:

- Log4shell (CVE-2021-44228, CVE-2021-45046): https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf

Siemens recommends to stay informed about updates of both SSA-661247 and SSA-501673.

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 (2021-12-19): Publication Date

## 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.