### SSA-661247: Apache Log4j Vulnerabilities (Log4Shell, CVE-2021-44228, CVE-2021-45046) - Impact to Siemens Products

**Publication Date:** 2021-12-13  
**Last Update:** 2021-12-15  
**Current Version:** V1.1  
**CVSS v3.1 Base Score:** 10.0

### SUMMARY

On 2021-12-09, a vulnerability in Apache Log4j (a logging tool used in many Java-based applications) was disclosed, that could allow remote unauthenticated attackers to execute code on vulnerable systems. The vulnerability is tracked as CVE-2021-44228 and is also known as “Log4Shell”.

On 2021-12-14 an additional denial of service vulnerability (CVE-2021-45046) was published rendering the initial mitigations and fix in version 2.15.0 as incomplete under certain non-default configurations. Log4j versions 2.16.0 and 2.12.2 are supposed to fix both vulnerabilities.

Siemens is currently 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.

### AFFECTED PRODUCTS AND SOLUTION

<table>
<thead>
<tr>
<th>Affected Product and Versions</th>
<th>Remediation</th>
</tr>
</thead>
</table>
| **Capital:**  
  All versions >= 2019.1 SP1912 only if Teamcenter integration feature is used | Currently no remediation is available  
  See further recommendations from section Workarounds and Mitigations |
| **Comos Desktop App:**  
  All versions | Currently no remediation is available  
  Uninstall “Teamcenter Client Communication System (TCSS)” or block both incoming and outgoing connections between the system and the Internet.  
  See further recommendations from section Workarounds and Mitigations |
| **Desigo CC Advanced Reporting:**  
  V4.0, V4.1, V4.2, V5.0, V5.1 | Currently no remediation is available  
  Block both incoming and outgoing connections between the system and the Internet.  
  See further recommendations from section Workarounds and Mitigations |
| **Desigo CC Info Center:**  
  V5.0, V5.1 | Currently no remediation is available  
  Block both incoming and outgoing connections between the system and the Internet.  
  See further recommendations from section Workarounds and Mitigations |
| **E-Car OC Cloud Application:**  
  All versions < 2021-12-13 | Vulnerability CVE-2021-44228 fixed on central cloud service starting 2021-12-13; no user actions necessary  
  See further recommendations from section Workarounds and Mitigations |
<table>
<thead>
<tr>
<th>Product/Software</th>
<th>Version Details</th>
<th>Mitigation Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>EnergyIP Prepay:</td>
<td>V3.7, V3.8</td>
<td>Specific mitigation information has been released for the customer projects with the request of immediate deployment. The long-term solution of updating the log4j2 component to a fix version is being tested and will be released, once confirmed being safe for the particular product version in line with the project Service Level Agreements. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>GMA-Manager:</td>
<td>All versions &gt; V8.6.2j-398</td>
<td>Currently no remediation is available. See recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>HES UDIS:</td>
<td>All versions</td>
<td>Currently no remediation is available. Specific mitigation information has been released for the local project teams with the request of immediate deployment. A patch is planned for the next regular release. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Industrial Edge Management App (IEM-App):</td>
<td>All versions</td>
<td>Exposure to vulnerability is limited as IEM-App runs in IEM-OS and IEM-OS is not intended to be exposed to public internet and should be operated in a protected environment. Please refer to the Industrial Edge - Security overview <a href="https://support.industry.siemens.com/cs/us/en/view/109804061">https://support.industry.siemens.com/cs/us/en/view/109804061</a>. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Industrial Edge Management OS (IEM-OS):</td>
<td>All versions</td>
<td>Exposure to vulnerability is limited as IEM-OS is not intended to be exposed to public internet and should be operated in a protected environment. Please refer to the Industrial Edge - Security overview: <a href="https://support.industry.siemens.com/cs/us/en/view/109804061">https://support.industry.siemens.com/cs/us/en/view/109804061</a>. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Industrial Edge Management Hub:</td>
<td>All versions</td>
<td>Vulnerability CVE-2021-44228 fixed on central cloud service starting 2021-12-13; no user actions necessary. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>LOGO! Soft Comfort:</td>
<td>All versions</td>
<td>Currently no remediation is available. Only LOGO! Web Projects that are deployed to AWS are potentially affected by this vulnerability. While the library is not used within the default configuration, it may be used within a project. To mitigate the vulnerability, set the JVM parameter LOG4J_FORMAT_MSG_NO_LOOKUPS to true in the environment configuration section of the AWS Elastic Beanstalk console of your AWS Instance. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Component</td>
<td>Versions</td>
<td>Recommendations</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| Mendix Applications           | All versions                      | Although the Mendix runtime itself is not vulnerable to this exploit, we nevertheless recommend to upgrade log4j-core to the latest available version if log4j-core is part of your project. This advice is regardless of the JRE/JDK version the app runs on.  
https://status.mendix.com/incidents/8j5043my610c  
See further recommendations from section Workarounds and Mitigations |
| Mindsphere Cloud Application  | All versions < 2021-12-11          | Vulnerability CVE-2021-44228 fixed on central cloud service starting 2021-12-11; no user actions necessary  
See further recommendations from section Workarounds and Mitigations |
| NX                            | All versions                      | Currently no remediation is available  
See further recommendations from section Workarounds and Mitigations |
| Opcenter Intelligence         | All versions >= 3.2 only OEM version that ships Tableau | Currently no remediation is available  
Set the JVM Parameter LOG4J_FORMAT_MSG_NO_LOOKUPS to true as described below  
See further recommendations from section Workarounds and Mitigations |
| Operation Scheduler           | All versions >= V1.1.3             | Currently no remediation is available  
Block both incoming and outgoing connections between the system and the Internet.  
See further recommendations from section Workarounds and Mitigations |
| SIGUARD DSA                   | V4.2, V4.3, V4.4                  | Adapt the client and computation node start-up batch scripts or shell scripts by adding -Dlog4j2.formatMsgNoLookups=true directly after the java statement.  
Adapt the application server start-up by adding -Dlog4j2.formatMsgNoLookups=true somewhere after the standalone.sh statement.  
Stop and restart the SIGUARD DSA processes.  
See further recommendations from section Workarounds and Mitigations |
| SIMATIC WinCC V7.4            | All versions < V7.4 SP1            | Update to V7.4 SP1 or later version  
Only connect to trusted OPC UA servers  
See further recommendations from section Workarounds and Mitigations |
<table>
<thead>
<tr>
<th>Product</th>
<th>Version Details</th>
<th>Remediation Available</th>
<th>Mitigation Steps</th>
</tr>
</thead>
<tbody>
<tr>
<td>SiPass integrated V2.80:</td>
<td>All versions</td>
<td>Currently no remediation available</td>
<td>Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>SiPass integrated V2.85:</td>
<td>All versions</td>
<td>Currently no remediation available</td>
<td>Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Siveillance Command:</td>
<td>All versions &gt;= 4.16.2.1</td>
<td>Currently no remediation available</td>
<td>Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Siveillance Control Pro:</td>
<td>All versions</td>
<td>Hotfix available for versions &gt;= V2.1 (please contact customer support)</td>
<td>Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Siveillance Identity V1.5:</td>
<td>All versions</td>
<td>Set the environment variable LOG4J_FORMAT_MSG_NO_LOOKUPS on the server to “true” and restart the Tomcat service.</td>
<td>Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Siveillance Identity V1.6:</td>
<td>All versions</td>
<td>Set the environment variable LOG4J_FORMAT_MSG_NO_LOOKUPS on the server to “true” and restart the Tomcat service.</td>
<td>Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Siveillance Vantage:</td>
<td>All versions</td>
<td>Currently no remediation available</td>
<td>Block both incoming and outgoing connections between the system and the Internet. See further recommendations from section Workarounds and Mitigations</td>
</tr>
<tr>
<td>Spectrum Power™ 4:</td>
<td>All versions only with component jROS in version 3.0.0</td>
<td>Update to V4.70 SP9 and apply the patch provided via customer support</td>
<td>See further recommendations from section Workarounds and Mitigations</td>
</tr>
</tbody>
</table>
### Spectrum Power™ 7:
- **All versions < V2.30 SP2 only with component jROS**
  - Update to V21Q4 and apply the patch provided via customer support
  - See further recommendations from section Workarounds and Mitigations

### Spectrum Power™ 7:
- **All versions >= V2.30 SP2**
  - Update to V21Q4 and apply the patch provided via customer support
  - See further recommendations from section Workarounds and Mitigations

### Teamcenter Suite:
- **All versions**
  - Currently no remediation is available
  - Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/PL8600700
  - See further recommendations from section Workarounds and Mitigations

### VeSys:
- **All versions >= 2019.1 SP1912 only if Teamcenter integration feature is used**
  - Currently no remediation is available
  - Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/MG618363
  - See further recommendations from section Workarounds and Mitigations

### Xpedition EDM Client:
- **VX.2.6 - VX.2.10**
  - Currently no remediation is available
  - Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/MG618343
  - See further recommendations from section Workarounds and Mitigations

### Xpedition EDM Server:
- **VX.2.6 - VX.2.10**
  - Currently no remediation is available
  - Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/MG618343
  - See further recommendations from section Workarounds and Mitigations

### Xpedition Package Integrator:
- **VX.2.6 - VX.2.10**
  - Currently no remediation is available
  - Find detailed mitigation steps at: https://support.sw.siemens.com/en-US/knowledge-base/MG618343
  - 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 the specific Siemens product allows it:** Set the parameter log4j2.formatMsgNoLookups to ‘true’. This measure reduces (but not completely eliminates) the risk for remote command execution via CVE-2021-44228. It does not mitigate CVE-2021-45046.

- **If the specific Siemens product allows it:** Remove the JndiLookup class from the classpath: ‘zip -q -d log4j-core-*.jar org/apache/logging/log4j/core/lookup/JndiLookup.class’. This measure mitigates both CVE-2021-44228 and CVE-2021-45046.

- **If the specific Siemens product allows it:** Modify all PatternLayout patterns to specify the message converter as ‘%m{nolookups}’ instead of just ‘%m’. This measure reduces (but not completely eliminates) the risk for remote command execution via CVE-2021-44228. It does not mitigate the risk for CVE-2021-45046.
CVE-2021-45046.

- If the specific Siemens product allows it: Update the Log4j component to 2.16.0 or later versions on the systems where the product is installed. This measure mitigates both CVE-2021-44228 and CVE-2021-45046.

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

Advantage Navigator is a cloud-based advanced analytics platform designed to help you optimize the performance of your buildings.

COMOS is an object oriented database system that supports collecting, processing, saving, and distributing information throughout the entire design process.

E-Car OC (E-Car Operation Center) is a cloud service that manages charging infrastructures for electric vehicles (EVs), both in domestic and public or semi-public areas.

EnergyIP applications enable utilities, retailers, DSO’s and market operators proven technology to meet the needs and requirements of the energy sector.

EnergyIP Prepay is an end-to-end solution for smart prepaid energy management. It features flexible tariff management, real-time rating and charging, convenient payment, and recharging options as well as intelligent energy consumption control features.

HES UDIS (Head-End System Universal Device Integration System) is an integrated solution for processing meter data and device events.

Industrial Edge Management (IEM) enables a centralized management of Siemens Industrial Edge Devices and Edge Applications. IEM is tailored to customer’s needs and is operated by the customer (on-premises).

LOGO! Soft Comfort is an engineering software to configure and program LOGO! BM (Base Module) devices.

Mendix is a high productivity app platform that enables you to build and continuously improve mobile and web applications at scale. The Mendix Platform is designed to accelerate enterprise app delivery across your entire application development lifecycle, from ideation to deployment and operations.

MindSphere is an industrial IoT as a service solution.

Opcenter Intelligence (formerly known as “Manufacturing Intelligence”) connects, organizes and aggregates manufacturing data from disparate company sources into cohesive, intelligent and contextualized information.

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

SIGUARD DSA is a model-based dynamic stability assessment tool for online control room use and offline operational planning purposes.

SIMATIC WinCC is a supervisory control and data acquisition (SCADA) system.

SiPass integrated is a powerful and extremely flexible access control system.
Siemens Security Advisory by Siemens ProductCERT

Siemens Control Pro is a command and control solution, specifically designed to support security management at critical infrastructure sites such as ports, airports, oil and gas power generation and distribution, chemical and pharma industries, heavy industries and campus environments.

Siveillance Vantage is an innovative and advanced software solution for mission critical security command and control centers operating critical infrastructure applications.

Solid Edge is a portfolio of software tools that addresses various product development processes: 3D design, simulation, manufacturing, and design management.

Spectrum Power provides basic components for SCADA, communications, and data modeling for control and monitoring systems. Application suites can be added to optimize network and generation management for all areas of energy management.

Teamcenter provides a digital twin of products to help the analysis and predict performance before investment in physical parts and production.

Xpedition is an innovative PCB design flow application, providing integration from system design definition to manufacturing execution.

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-2021-44228

Apache Log4j V2, versions < 2.15.0 do not protect JNDI features (as used in configuration, log messages, and parameters) against attacker controlled LDAP and other JNDI related endpoints.

An attacker who can control log messages or log message parameters could execute arbitrary code loaded from LDAP servers when message lookup substitution is enabled.

CVSS v3.1 Base Score 10.0
CWE CWE-20: Improper Input Validation

Vulnerability CVE-2021-45046

The fix to address CVE-2021-44228 was incomplete in certain non-default configurations, when the logging configuration uses a non-default Pattern Layout with either a Context Lookup (for example, $ctx:loginId) or a Thread Context Map pattern (%X, %mdc, or %MDC).

This could allow attackers with control over Thread Context Map (MDC) input data to craft malicious input data using a JNDI Lookup pattern resulting in a denial of service (DOS) attack.

CVSS v3.1 Base Score 3.7
CWE CWE-20: Improper Input Validation

ADDITIONAL INFORMATION

This advisory will be updated as more information becomes available.

SSA-661247 © Siemens 2021
The following Siemens products are under active investigation to determine whether they are affected:

- Advantage Navigator Cloud Service
- Advantage Navigator Software Proxy
- Comfy / Enlighted
- EnergyIP

For more details regarding the Log4j vulnerabilities refer to [https://logging.apache.org/log4j/2.x/security.html](https://logging.apache.org/log4j/2.x/security.html)

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

[https://www.siemens.com/cert/advisories](https://www.siemens.com/cert/advisories)

**HISTORY DATA**

V1.0 (2021-12-13): Publication Date
V1.1 (2021-12-15): Added additional (potentially) affected products and additional remediation or mitigation measures; added reference to CVE-2021-45046 and updated mitigations accordingly

**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](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.