

## **SSA-371761: Arbitrary Code Execution Vulnerability in the Logback Component of SINEC NMS before V1.0.3**

Publication Date: 2022-11-08  
Last Update: 2022-11-08  
Current Version: V1.0  
CVSS v3.1 Base Score: 6.6

### **SUMMARY**

SINEC NMS versions before V1.0.3 are affected by a vulnerability in the logback component (CVE-2021-42550) that could allow attackers with write access to the logback configuration file to execute arbitrary code on the system.

Siemens has released an update for SINEC NMS and recommends to update to the latest version.

### **AFFECTED PRODUCTS AND SOLUTION**

<b>Affected Product and Versions</b>	<b>Remediation</b>
SINEC NMS: All versions < V1.0.3	Update to V1.0.3 or later version <a href="https://support.industry.siemens.com/cs/ww/en/view/109813788/">https://support.industry.siemens.com/cs/ww/en/view/109813788/</a> See further recommendations from section <a href="#">Workarounds and Mitigations</a>

### **WORKAROUNDS AND MITIGATIONS**

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

- Restrict the write access to the logback configuration file (logback.xml) to trusted personnel

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**

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.

## **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-2021-42550**

In logback version 1.2.7 and prior versions, an attacker with the required privileges to edit configurations files could craft a malicious configuration allowing to execute arbitrary code loaded from LDAP servers.

CVSS v3.1 Base Score	6.6
CVSS Vector	<a href="#">CVSS:3.1/AV:N/AC:H/PR:H/UI:N/S:U/C:H/I:H/A:H</a>
CWE	CWE-502: Deserialization of Untrusted Data

## **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 (2022-11-08): 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](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.