SSA-789345: Code Execution Vulnerabilities in Siveillance Video Event and Management Servers

Publication Date: 2023-05-09
Last Update: 2023-05-09
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

Both the Event Server and the Management Server components of Siveillance Video deserialize data without sufficient validations. This could allow an authenticated remote attacker to execute code on the affected system.

Siemens has released updates for the affected products and recommends to update to the latest versions. The provided cumulative hotfix releases include the fixes for both Event Server (ES) and Management Server (MS). Ensure to apply the fixes on all relevant servers in your deployment.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance Video 2020 R2: All versions < V20.2 HotfixRev14	Update to V20.2 HotfixRev14 or later version https://support.industry.siemens.com/cs/ww/en/view/109781128/
Siveillance Video 2020 R3: All versions < V20.3 HotfixRev12	Update to V20.3 HotfixRev12 or later version https://support.industry.siemens.com/cs/ww/en/view/109791980/
Siveillance Video 2021 R1: All versions < V21.1 HotfixRev12	Update to V21.1 HotfixRev12 or later version https://support.industry.siemens.com/cs/ww/en/view/109801904/
Siveillance Video 2021 R2: All versions < V21.2 HotfixRev8	Update to V21.2 HotfixRev8 or later version https://support.industry.siemens.com/cs/ww/en/view/109805466/
Siveillance Video 2022 R1: All versions < V22.1 HotfixRev7	Update to V22.1 HotfixRev7 or later version https://support.industry.siemens.com/cs/ww/en/view/109810201/
Siveillance Video 2022 R2: All versions < V22.2 HotfixRev5	Update to V22.2 HotfixRev5 or later version https://support.industry.siemens.com/cs/ww/en/view/109812608/
Siveillance Video 2022 R3: All versions < V22.3 HotfixRev2	Update to V22.3 HotfixRev2 or later version https://support.industry.siemens.com/cs/ww/en/view/109815353/

Siveillance Video 2023 R1: All versions < V23.1 HotfixRev1	Update to V23.1 HotfixRev1 or later version https://support.industry.siemens.com/cs/ww/en/view/109820659/

WORKAROUNDS AND MITIGATIONS

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 affected products with appropriate mechanisms. It is advised to follow recommended security practices in order to run the devices in a protected IT environment.

PRODUCT DESCRIPTION

Siveillance Video (formerly called Siveillance VMS) is a powerful IP video management software designed for deployments ranging from small and simple to large-scale and high-security. The Siveillance Video portfolio consists of four versions, Siveillance Video Core, Core Plus, Advanced, and Pro, addressing the specific needs of small and medium size solutions up to large complex deployments.

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-2023-30898

The Event Server component of affected applications deserializes data without sufficient validations. This could allow an authenticated remote attacker to execute code on the affected system.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

Vulnerability CVE-2023-30899

The Management Server component of affected applications deserializes data without sufficient validations. This could allow an authenticated remote attacker to execute code on the affected system.

CVSS v3.1 Base Score	9.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-502: Deserialization of Untrusted Data

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Milestone PSIRT for reporting and coordinated disclosure

ADDITIONAL INFORMATION

The provided cumulative hotfix releases include the fixes for both Event Server (ES) and Management Server (MS). Ensure to apply the fixes on all relevant servers in your deployment.

For additional information regarding the vulnerabilities see the related Milestone Security Advisories:

- Event Server: https://supportcommunity.milestonesys.com/s/article/Milestone-ES-possible-Remote-Code-Execution-by-authenticated-user
- Management Server: https://supportcommunity.milestonesys.com/s/article/Milestone-MS-possible-Remote-Code-Execution-by-authenticated-user

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 (2023-05-09):	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.