SSA-640732: Authentication Bypass Vulnerability in Siveillance Video Mobile Server

Publication Date:	2022-10-21
Last Update:	2022-10-21
Current Version:	V1.0
CVSS v3.1 Base Score:	9.4

SUMMARY

The mobile server component of Siveillance Video 2022 R2 contains an authentication bypass vulnerability that could allow an unauthenticated remote attacker to access the application without a valid account.

Siemens has released a hotfix for Siveillance Video 2022 R2 and recommends to apply the hotfix on all installations of the mobile server.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Siveillance Video Mobile Server V2022 R2: All versions < V22.2a (80)	Update to V22.2a (80) or later version by applying the latest hotfix of the Mobile Server Installer (Vulnerability Hotfix) https://support.industry.siemens.com/cs/ww/en/view/109812608/ 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:

- Enable the feature “Servers > Mobile Servers > Deny the built-in Administrators role access to the mobile servers” for all configured mobile servers

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-2022-43400

The mobile server component of affected applications improperly handles the log in for Active Directory accounts that are part of Administrators group.

This could allow an unauthenticated remote attacker to access the application without a valid account.

CVSS v3.1 Base Score	9.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-1390: Weak Authentication

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Milestone PSIRT for reporting and coordinated disclosure

ADDITIONAL INFORMATION

For additional information regarding this vulnerability see the related Milestone Security Advisory at https://supportcommunity.milestonesys.com/s/article/Milestone-Mobile-Server-authentication-bypass-vulnerability.

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 (2022-10-21):	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.