SSA-761617: Authentication Bypass and Information Disclosure Vulnerabilities in SiNVR/SiVMS Video Server

Publication Date: 2019-12-10
Last Update: 2024-01-09
Current Version: V1.2
CVSS v3.1 Base Score: 9.8

SUMMARY

The Video Server application in SiNVR/SiVMS solutions contains two vulnerabilities involving authentication bypass (CVE-2019-18339) and information disclosure (CVE-2019-18340).

PKE has released an update of the application that fixes CVE-2019-18339. This update is not available under the former Siemens OEM brand name SiNVR. For details contact PKE (https://pke.at/).

Siemens recommends specific countermeasures to mitigate the vulnerabilities.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SiNVR/SiVMS Video Server: All versions < V5.0.0	Update to V5.0.0 or later version See further recommendations from section Workarounds and Mitigations
SiNVR/SiVMS Video Server: All versions >= V5.0.0 affected by CVE-2019-18340	Currently no fix is planned See 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:

- Apply ACL/firewall configuration on the Video Servers to ensure that only legitimate systems are able to access the configured server ports. Harden all systems accordingly to prevent unauthorized access
- CVE-2019-18339: SiNVR/SiVMS deployments with active Control Center Server (CCS) should ensure that every video server and client has the Authorization Server set to “Control Center Server” (Configuration -> Appearance -> Desktop -> Authorization Server)
- CVE-2019-18340: Harden the Video Servers to prevent local access by unauthorized users

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

The Control Center Server (CCS) is the optional central server component of PKE management solutions (e.g., SiNVR/SiVMS). The CCS combines all centralized tasks within a server, such as database access or user management.

SiNVR is the Siemens OEM version of SiVMS, a video management solution acquired by PKE Deutschland GmbH and formerly distributed by Schille Informationssysteme GmbH. SiNVR/SiVMS is not to be confused with the product Siveillance VMS. Note that SiNVR is no longer distributed or supported by Siemens beyond version 3.

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-2019-18339

The HTTP service (default port 5401/tcp) of the SiVMS/SiNVR Video Server contains an authentication bypass vulnerability, even when properly configured with enforced authentication.

A remote attacker with network access to the Video Server could exploit this vulnerability to read the SiVMS/SiNVR users database, including the passwords of all users in obfuscated cleartext.

CVSS v3.1 Base Score	9.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:F/RL:U/RC:C
CWE	CWE-306: Missing Authentication for Critical Function

Vulnerability CVE-2019-18340

Both the SiVMS/SiNVR Video Server and the Control Center Server (CCS) store user and device passwords by applying weak cryptography.

A local attacker could exploit this vulnerability to extract the passwords from the user database and/or the device configuration files to conduct further attacks.

CVSS v3.1 Base Score	5.5
CVSS Vector	CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:N/A:N/E:F/RL:U/RC:C
CWE	CWE-327: Use of a Broken or Risky Cryptographic Algorithm

ACKNOWLEDGMENTS

Siemens thanks the following party for its efforts:

- Raphaël Rigo from Airbus Security Lab for reporting the vulnerabilities

ADDITIONAL INFORMATION

The links to vendor advisory and software downloads no longer exist. For support contact PKE (https://pke.at/).

All vulnerabilities that were reported in V1.0 of this advisory, but only apply to the Control Center Server (CCS) have been removed and are now addressed in this advisory: SSA-761844, initial release on 2021-04-13.

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 (2019-12-10):	Publication Date
V1.1 (2021-04-13):	Added partial solution for SiNVR/SiVMS Video Server; removed information for Control Center Server (CCS), which is now addressed in SSA-761844
V1.2 (2024-01-09):	Cleanup: removed orphaned links to vendor advisories and software downloads

TERMS OF USE