SSA-761617: Multiple Vulnerabilities in SiNVR Video Management Solution

Publication Date: 2019-12-10
Last Update: 2019-12-10
Current Version: V1.0
CVSS v3.1 Base Score: 9.9

SUMMARY

SiNVR V3 contains seven vulnerabilities in the components Video Server and Central Control Server (CCS), involving authentication bypass (CVE-2019-18337, CVE-2019-18339, CVE-2019-18341), information disclosure (CVE-2019-13947, CVE-2019-18340), path traversal (CVE-2019-18338), and privilege escalation (CVE-2019-18342). Siemens recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SiNVR 3 Central Control Server (CCS): all versions	See recommendations from section Workarounds and Mitigations
SiNVR 3 Video Server: all versions	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:

- General - Apply ACL/firewall configuration on the SiNVR Video and CCS servers to ensure that only legitimate SiNVR systems are able to access the configured Video/CCS server ports. Harden all SiNVR systems accordingly to prevent unauthorized access. Consider to apply encryption and authentication on the network (e.g., via TLS on application level or via IPSec on host level).
- CVE-2019-18338, CVE-2019-18341, CVE-2019-18342 - Limit the access of the CCS server application to other applications that are not part of it.
- CVE-2019-18339 - SiNVR deployments with active CCS should ensure that every SiNVR server and client has the Authorization Server set to “Control Center Server” (Configuration -> Appearance -> Desktop -> Authorization Server).
- CVE-2019-18340 - Harden the SiNVR Video servers and CCS server to prevent local access by unauthorized users.
- CVE-2019-13947 - Disable the web interface of CCS if not used. Alternatively, restrict access from localhost only, or only to trusted hosts of CCS administrators. Enable TLS for the web interface of CCS.

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

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.

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-2019-13947

The user configuration menu in the web interface of the SiNVR 3 Central Control Server (CCS) transfers user passwords in clear to the client (browser).

An attacker with administrative privileges for the web interface could be able to read (and not only reset) passwords of other SiNVR 3 CCS users.

CVSS v3.1 Base Score	4.9
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:N/A:N/E:F/RL:U/RC:C
CWE	CWE-317: Cleartext Storage of Sensitive Information in GUI

Vulnerability CVE-2019-18337

The SiNVR 3 Central Control Server (CCS) contains an authentication bypass vulnerability in its XML-based communication protocol as provided by default on ports 5444/tcp and 5440/tcp.

A remote attacker with network access to the CCS server could exploit this vulnerability to read the CCS 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-287: Improper Authentication

Vulnerability CVE-2019-18338

The SiNVR 3 Central Control Server (CCS) contains a directory traversal vulnerability in its XML-based communication protocol as provided by default on ports 5444/tcp and 5440/tcp.

An authenticated remote attacker with network access to the CCS server could exploit this vulnerability to list arbitrary directories or read files outside of the CCS application context.

CVSS v3.1 Base Score	7.7
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:N/A:N/E:F/RL:U/RC:C
CWE	CWE-23: Relative Path Traversal

Vulnerability CVE-2019-18339

The HTTP service (default port 5401/tcp) of the SiNVR 3 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 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 SiNVR 3 Video Server and the Central Control 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-261: Weak Cryptography for Passwords

Vulnerability CVE-2019-18341

The SFTP service (default port 22/tcp) of the SiNVR 3 Central Control Server (CCS) contains an authentication bypass vulnerability.

A remote attacker with network access to the CCS server could exploit this vulnerability to read data from the EDIR directory (for example, the list of all configured stations).

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:F/RL:U/RC:C
CWE	CWE-287: Improper Authentication

Vulnerability CVE-2019-18342

The SFTP service (default port 22/tcp) of the SiNVR 3 Central Control Server (CCS) does not properly limit its capabilities to the specified purpose.

In conjunction with CVE-2019-18341, an unauthenticated remote attacker with network access to the CCS server could exploit this vulnerability to read or delete arbitrary files, or access other resources on the same server.

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:F/RL:U/RC:C
CWE	CWE-749: Exposed Dangerous Method or Function

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Raphaël Rigo from Airbus Security Lab for reporting vulnerabilities CVE-2019-18337 through CVE-2019-18340

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 (2019-12-10): 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.