SSA-844761: Multiple Vulnerabilities in SiNVR/SiVMS Video Server

Publication Date: 2020-03-10
Last Update: 2024-01-09
Current Version: V1.3
CVSS v3.1 Base Score: 7.5

SUMMARY

The Video Server application in SiNVR/SiVMS solutions contains five vulnerabilities involving information disclosure (CVE-2019-19291, CVE-2019-19299), path traversal (CVE-2019-19296, CVE-2019-19297), and denial-of-service (CVE-2019-19298).

PKE has released updates of the application that fixes the reported vulnerabilities, except for CVE-2019-19299. This update is not available under the former Siemens OEM brand name SiNVR. For details contact PKE (https://pke.at/).

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 < V5.0.2 affected by CVE-2019-19298, CVE-2019-19299	Update to V5.0.2 or later version See further recommendations from section Workarounds and Mitigations
SiNVR/SiVMS Video Server: All versions >= V5.0.2 affected by CVE-2019-19299	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 Consider to apply encryption and authentication on the network (e.g., via TLS on application level or via IPSec on host level)
- CVE-2019-19291, CVE-2019-19296: Disable the two FTP services of the Video Server
- CVE-2019-19298: The update to V5.0.2 also provides an additional authentication feature that allows to protect the access to the streaming service via individual account names and passwords for every stream recorder. It is recommended to configure this feature accordingly. For details see the release notes of V5.0.2

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-2019-19291

The FTP services of the SiVMS/SiNVR Video Server and the Control Center Server (CCS) maintain log files that store login credentials in cleartext. In configurations where the FTP service is enabled, authenticated remote attackers could extract login credentials of other users of the service.

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-313: Cleartext Storage in a File or on Disk

Vulnerability CVE-2019-19296

The two FTP services (default ports 21/tcp and 5411/tcp) of the SiVMS/SiNVR Video Server contain a path traversal vulnerability that could allow an authenticated remote attacker to access and download arbitrary files from the server, if the FTP services are enabled.

CVSS v3.1 Base Score	6.8
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:N/E:P/RL:U/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2019-19297

The streaming service (default port 5410/tcp) of the SiVMS/SiNVR Video Server contains a path traversal vulnerability, that could allow an unauthenticated remote attacker to access and download arbitrary files from the server.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')

Vulnerability CVE-2019-19298

The streaming service (default port 5410/tcp) of the SiVMS/SiNVR Video Server contains a input validation vulnerability, that could allow an unauthenticated remote attacker to cause a Denial-of-Service condition by sending malformed HTTP requests.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H/E:P/RL:U/RC:C
CWE	CWE-20: Improper Input Validation

Vulnerability CVE-2019-19299

The streaming service (default port 5410/tcp) of the SiVMS/SiNVR Video Server applies weak cryptography when exposing device (camera) passwords. This could allow an unauthenticated remote attacker to read and decrypt the passwords and conduct further attacks.

CVSS v3.1 Base Score	7.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N/E:P/RL:U/RC:C
CWE	CWE-326: Inadequate Encryption Strength

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 addressed in SSA-761844 (https://cert-portal.siemens.com/productcert/html/ssa-761844.html), 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 (2020-03-10):	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 (2021-08-10):	Added solution for CVE-2019-19298 and related additional security hardening measures
V1.3 (2024-01-09):	Cleanup: removed orphaned links to vendor advisories and software downloads

TERMS OF USE