# SSA-844761: Multiple Vulnerabilities in CCS, FTP and Streaming Services of SiNVR Video Management Solution

Publication Date: 2020-03-10
Last Update: 2020-03-10
Current Version: V1.0
CVSS v3.1 Base Score: 8.8

## SUMMARY

SiNVR V3 contains several vulnerabilities in the components Central Control Server (CCS), as well as in the FTP and streaming services of the Video Server. The vulnerabilities involve path traversal (CVE-2019-19290, CVE-2019-19296, CVE-2019-19297), information disclosure (CVE-2019-19291, CVE-2019-19299), SQL injection (CVE-2019-19292), cross-site scripting (CVE-2019-19293, CVE-2019-19294), insufficient logging (CVE-2019-19295), and denial-of-service (CVE-2019-19298).

Siemens recommends specific countermeasures until fixes are available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SiNVR 3 Central Control Server (CCS):<br>all versions | See recommendations from section Workarounds and Mitigations |
| SiNVR 3 Video Server:<br>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 (applies to all vulnerabilities listed in this advisory) - 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-2019-19290, CVE-2019-19293, CVE-2019-19294 - 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.
- CVE-2019-19291 - Disable the FTP service of the CCS
- CVE-2019-19296 - Disable the two FTP services of the Video Server

## 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-2019-19290

The DOWNLOADS section in the web interface of the SiNVR 3 Central Control Server (CCS) contains a path traversal vulnerability that could allow an authenticated remote attacker to access and download arbitrary files from the server where CCS is installed.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.5 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/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-2019-19291

The FTP service of the SiNVR 3 Central Control Server (CCS) maintains a log file that stores 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-2019-19292

The SiNVR 3 Central Control Server (CCS) contains an SQL injection vulnerability in its XML-based communication protocol as provided by default on ports 5444/tcp and 5440/tcp. An authenticated remote attacker could exploit this vulnerability to read or modify the CCS database and potentially execute administrative database operations or operating system commands.

| | |
|---|---|
| CVSS v3.1 Base Score | 8.8 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:U/RC:C |
| CWE | CWE-89: Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') |

Vulnerability CVE-2019-19293

The web interface of the SiNVR 3 Central Control Server (CCS) contains a reflected Cross-site Scripting (XSS) vulnerability that could allow an unauthenticated remote attacker to steal sensitive data or execute administrative actions on behalf of a legitimate administrator of the CCS web interface.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.1 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:R/S:C/C:N/I:H/A:N/E:P/RL:U/RC:C |
| CWE | CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

Vulnerability CVE-2019-19294

The web interface of the SiNVR 3 Central Control Server (CCS) contains multiple stored Cross-site Scripting (XSS) vulnerabilities in several input fields. This could allow an authenticated remote attacker to inject malicious JavaScript code into the CCS web application that is later executed in the browser context of any other user who views the relevant CCS web content.

| | |
|---|---|
| CVSS v3.1 Base Score | 6.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:C/C:N/I:H/A:N/E:P/RL:U/RC:C |
| CWE | CWE-79: Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') |

Vulnerability CVE-2019-19295

The SiNVR 3 Central Control Server (CCS) does not enforce logging of security-relevant activities in its XML-based communication protocol as provided by default on ports 5444/tcp and 5440/tcp. An authenticated remote attacker could exploit this vulnerability to perform covert actions that are not visible in the application log.

| | |
|---|---|
| CVSS v3.1 Base Score | 4.3 |
| CVSS Vector | CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:L/A:N/E:P/RL:U/RC:C |
| CWE | CWE-778: Insufficient Logging |

Vulnerability CVE-2019-19296

The two FTP services (default ports 21/tcp and 5411/tcp) of the SiNVR 3 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 SiNVR 3 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 SiNVR 3 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 requeats.

| | |
|---|---|
| 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 SiNVR 3 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-261: Weak Cryptography for Passwords |

## 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 (2020-03-10): 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.