

## SSA-761844: Multiple Vulnerabilities in Control Center Server (CCS)

Publication Date: 2021-04-13  
Last Update: 2024-01-09  
Current Version: V1.1  
CVSS v3.1 Base Score: 9.9

### SUMMARY

The advisory informs about multiple vulnerabilities in the Central Control Server (CCS) application, as initially reported in SSA-761617 (<https://cert-portal.siemens.com/productcert/html/ssa-761617.html>) on 2019-12-10 and SSA-844761 (<https://cert-portal.siemens.com/productcert/html/ssa-844761.html>) on 2020-03-10.

The vulnerabilities involve authentication bypass (CVE-2019-18337, CVE-2019-18341), path traversal (CVE-2019-18338, CVE-2019-19290), information disclosure (CVE-2019-13947, CVE-2019-18340, CVE-2019-19291), privilege escalation (CVE-2019-18342), SQL injection (CVE-2019-19292), cross-site scripting (CVE-2019-19293, CVE-2019-19294), and insufficient logging (CVE-2019-19295).

PKE has released an update for CCS that fixes the reported vulnerabilities, except for CVE-2019-18340. For details contact PKE (<https://pke.at/>).

Siemens recommends to update to the latest version and recommends specific countermeasures to mitigate the vulnerabilities.

### AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Control Center Server (CCS): All versions < V1.5.0	Update to V1.5.0 or later version See further recommendations from section <a href="#">Workarounds and Mitigations</a>
Control Center Server (CCS): All versions >= V1.5.0 affected by CVE-2019-18340	Currently no fix is planned See recommendations from section <a href="#">Workarounds and Mitigations</a>

### 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 CCS server to ensure that only legitimate systems are able to access the configured CCS server ports. Harden the CCS server 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-2019-18340: Harden the CCS server to prevent local access by unauthorized users
- 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

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-2019-13947**

The user configuration menu in the web interface of the Control Center 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 CCS users.

CVSS v3.1 Base Score	4.9
CVSS Vector	<a href="#">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</a>
CWE	CWE-317: Cleartext Storage of Sensitive Information in GUI

### **Vulnerability CVE-2019-18337**

The Control Center 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	<a href="#">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</a>
CWE	CWE-287: Improper Authentication

### **Vulnerability CVE-2019-18338**

The Control Center 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-2019-18340**

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

### **Vulnerability CVE-2019-18341**

The SFTP service (default port 22/tcp) of the Control Center 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 Control Center 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

### **Vulnerability CVE-2019-19290**

The DOWNLOADS section in the web interface of the Control Center 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 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-2019-19292**

The Control Center 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 Control Center 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 Control Center 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 Control Center 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

## **ACKNOWLEDGMENTS**

Siemens thanks the following party for its efforts:

- Raphaël Rigo from Airbus Security Lab for reporting vulnerabilities CVE-2019-18337, CVE-2019-18338, and CVE-2019-18340

## **ADDITIONAL INFORMATION**

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

The vulnerabilities were initially reported in SSA-761617 (<https://cert-portal.siemens.com/productcert/html/ssa-761617.html>) on 2019-12-10 and SSA-844761 (<https://cert-portal.siemens.com/productcert/html/ssa-844761.html>) on 2020-03-10, along with other vulnerabilities that affect the SiNVR/SiVMS Video Server. To provide more clarity, the vulnerabilities that apply to CCS have been moved to this new advisory. The former advisories address the SiNVR/SiVMS Video Server only.

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 (2021-04-13): Publication Date

V1.1 (2024-01-09): Cleanup: removed orphaned links to vendor advisories and software downloads

## **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](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.