SSA-940818: UltraVNC Vulnerabilities in SIMATIC HMIs/WinCC Products

Publication Date: 2021-05-11
Last Update: 2021-05-11
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

UltraVNC vulnerabilities in the affected products listed below could allow remote code execution, information disclosure and Denial-of-Service attacks under certain conditions.

Siemens has released updates for the affected products and recommends to update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants): All versions < V16 Update 4	Update SIMATIC WinCC (TIA Portal) to V16 Update 4 or later version, and then update panel to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions < V16 Update 4	Update SIMATIC WinCC (TIA Portal) to V16 Update 4 or later version, and then update panel to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/
SIMATIC HMI KTP Mobile Panels KTP400F, KTP700, KTP700F, KTP900 and KTP900F: All versions < V16 Update 4	Update SIMATIC WinCC (TIA Portal) to V16 Update 4 or later version, and then update panel to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109775861/
SIMATIC WinCC Runtime Advanced: All versions < V16 Update 4	Update to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109776018/

WORKAROUNDS AND MITIGATIONS

Siemens has identified the following specific workarounds and mitigations that customers can apply to reduce the risk:

- Restrict access to port 5900/tcp to trusted IP addresses only

GENERAL SECURITY RECOMMENDATIONS

As a general security measure, Siemens strongly recommends to protect network access to devices with appropriate mechanisms. In order to operate the devices in a protected IT environment, Siemens recommends to configure the environment according to Siemens' operational guidelines for Industrial Security (Download: https://www.siemens.com/cert/operational-guidelines-industrial-security), and to follow the recommendations in the product manuals.

Additional information on Industrial Security by Siemens can be found at: https://www.siemens.com/industrialsecurity

PRODUCT DESCRIPTION

SIMATIC WinCC Runtime Advanced is a visualization runtime platform used for operator control and monitoring of machines and plants.

SIMATIC HMI Panels are used for operator control and monitoring of machines and plants.

SIPLUS extreme products are designed for reliable operation under extreme conditions and are based on SIMATIC, LOGO!, SITOP, SINAMICS, SIMOTION, SCALANCE or other devices. SIPLUS devices use the same firmware as the product they are based on.

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-2019-8259

UltraVNC revision 1198 contains multiple memory leaks in VNC client code, which could allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This vulnerability appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1199.

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:O/RC:C
CWE	CWE-665: Improper Initialization

Vulnerability CVE-2019-8260

UltraVNC revision 1199 has a out-of-bounds read vulnerability in VNC client RRE decoder code, caused by multiplication overflow. This vulnerability appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1200.

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:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2019-8261

UltraVNC revision 1199 has a out-of-bounds read vulnerability in VNC code inside client CoRRE decoder, caused by multiplication overflow. This vulnerability appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1200.

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:P/RL:O/RC:C
CWE	CWE-125: Out-of-bounds Read

Vulnerability CVE-2019-8262

UltraVNC revision 1203 has multiple heap buffer overflow vulnerabilities in VNC client code inside Ultra decoder, which could result in code execution. This vulnerability appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1204.

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:P/RL:O/RC:C
CWE	CWE-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-8263

UltraVNC revision 1205 has a stack-based buffer overflow vulnerability in VNC client code inside ShowConnInfo routine, which could lead to a denial of service (DoS) condition. This vulnerability appear to be exploitable via network connectivity. User interaction is required to trigger this vulnerability. This vulnerability has been fixed in revision 1206.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2019-8264

UltraVNC revision 1203 has a out-of-bounds access vulnerability in VNC client inside Ultra2 decoder, which can potentially result in code execution. This vulnerability appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.

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:P/RL:O/RC:C
CWE	CWE-788: Access of Memory Location After End of Buffer

Vulnerability CVE-2019-8265

UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of SETPIXELS macro in VNC client code, which can potentially result in code execution. This vulnerability appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1208.

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:P/RL:O/RC:C
CWE	CWE-788: Access of Memory Location After End of Buffer

Vulnerability CVE-2019-8275

UltraVNC revision 1211 has multiple improper null termination vulnerabilities in VNC server code, which could result in out-of-bound data being accessed by remote users. This vulnerability appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.

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:P/RL:O/RC:C
CWE	CWE-170: Improper Null Termination

Vulnerability CVE-2019-8277

UltraVNC revision 1211 contains multiple memory leaks in VNC server code, which could allow an attacker to read stack memory and can be abused for information disclosure. Combined with another vulnerability, it can be used to leak stack memory and bypass ASLR. This vulnerability appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1212.

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:O/RC:C
CWE	CWE-665: Improper Initialization

Vulnerability CVE-2019-8280

UltraVNC revision 1203 has out-of-bounds access vulnerability in VNC client inside RAW decoder, which can potentially result in code execution. This vulnerability appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1204.

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:P/RL:O/RC:C
CWE	CWE-788: Access of Memory Location After End of Buffer

ADDITIONAL INFORMATION

The vulnerabilities listed in this Siemens Security Advisory are part of a Kaspersky report. See VNC vulnerability research for related security advisories and additional information on the vulnerabilities.

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 (2021-05-11): Publication Date

TERMS OF USE