SSA-927095: UltraVNC Vulnerabilities in SINUMERIK Products

Publication Date:	2020-06-09
Last Update:	2020-06-09
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

UltraVNC (V1.2.2.3 and below) vulnerabilities in the affected products 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 that customers update to the latest versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK Access MyMachine /P2P: All versions < V4.8	Update to V4.8 SINUMERIK software can be obtained from your local Siemens account manager
SINUMERIK PCU base Win10 software /IPC: All versions < V14.00	Update to V14.00 SINUMERIK software can be obtained from your local Siemens account manager
SINUMERIK PCU base Win7 software /IPC: All versions < V12.01 HF4	Update to V12.01 HF4 SINUMERIK software can be obtained from your local Siemens account manager

WORKAROUNDS AND MITIGATIONS

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

- Restrict access to the device to the internal or VPN network and 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

SINUMERIK PCU (Panel Control Unit) base software /IPC provides SINUMERIK PCU functionality on defined SIMATIC IPCs.

SINUMERIK Access MyMachine P2P supports the commissioning of machines with SINUMERIK Operate, using a standard Windows PC.

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-2018-15361

UltraVNC revision 1198 has a buffer underflow vulnerability in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1199.

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-124: Buffer Underwrite ('Buffer Underflow')

Vulnerability CVE-2019-8258

UltraVNC revision 1198 has a heap buffer overflow vulnerability in VNC client code which results code execution. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1199.

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-2019-8259

UltraVNC revision 1198 contains multiple memory leaks in VNC client code, which 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 attack 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 attack 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 attack 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 results in code execution. This attack 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 stack-based buffer overflow vulnerability in VNC client code inside ShowConnInfo routine, which leads to a denial of service (DoS) condition. This attack 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 out-of-bounds access vulnerability in VNC client inside Ultra2 decoder, which can potentially result in code execution. This attack 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 attack 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-2019-8266

UltraVNC revision 1207 has multiple out-of-bounds access vulnerabilities connected with improper usage of ClientConnection::Copybuffer function in VNC client code, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. User interaction is required to trigger these vulnerabilities. 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-2019-8267

UltraVNC revision 1207 has out-of-bounds read vulnerability in VNC client code inside TextChat module, which results in a denial of service (DoS) condition. This attack appears to be exploitable via network connectivity. This vulnerability has been fixed in revision 1208.

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

Vulnerability CVE-2019-8268

UltraVNC revision 1206 has multiple off-by-one vulnerabilities in VNC client code connected with improper usage of ClientConnection::ReadString function, which can potentially result code execution. This attack appears to be exploitable via network connectivity. These vulnerabilities have been fixed in revision 1207.

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-193: Off-by-one Error

Vulnerability CVE-2019-8269

UltraVNC revision 1206 has stack-based Buffer overflow vulnerability in VNC client code inside FileTransfer module, which leads to a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1207.

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:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2019-8270

UltraVNC revision 1210 has out-of-bounds read vulnerability in VNC client code inside Ultra decoder, which results in a denial of service (DoS) condition. This attack appear to be exploitable via network connectivity. This vulnerability has been fixed in revision 1211.

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

Vulnerability CVE-2019-8271

UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer handler, which can potentially result code execution. This attack appears to be exploitable via network connectivity. This vulnerability has 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-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-8272

UltraVNC revision 1211 has multiple off-by-one vulnerabilities in VNC server code, which can potentially result in code execution. This attack 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-193: Off-by-one Error

Vulnerability CVE-2019-8273

UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer request handler, which can potentially result in code execution. This attack appears to be exploitable via network connectivity. This vulnerability has 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-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-8274

UltraVNC revision 1211 has a heap buffer overflow vulnerability in VNC server code inside file transfer offer handler, which can potentially in result code execution. This attack appears to be exploitable via network connectivity. This vulnerability has 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-122: Heap-based Buffer Overflow

Vulnerability CVE-2019-8275

UltraVNC revision 1211 has multiple improper null termination vulnerabilities in VNC server code, which result in out-of-bound data being accessed by remote users. This attack 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-2019-8276

UltraVNC revision 1211 has a stack buffer overflow vulnerability in VNC server code inside file transfer request handler, which can result in Denial of Service (DoS). This attack appears to be exploitable via network connectivity. This vulnerability has 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:N/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-121: Stack-based Buffer Overflow

Vulnerability CVE-2019-8277

UltraVNC revision 1211 contains multiple memory leaks in VNC server code, which allows 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 attack 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 code execution. This attack 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

Listed vulnerabilities are part of a Kaspersky report. See VNC vulnerability research for related security advisories and additional information on the vulnerabilites.

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 (2020-06-09): 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.