SSA-286838: Multiple Vulnerabilities in SINAMICS Medium Voltage Products

Publication Date: 2021-05-11
Last Update: 2021-08-10
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

SUMMARY

SINAMICS medium voltage products, with Sm@rtServer enabled on SIMATIC comfort HMI Panels, are affected by multiple vulnerabilities that could allow an attacker, under certain conditions, to gain full remote access to the HMI. Note that by default Sm@rtServer is disabled, but it can be enabled by the system integrator on request.

Siemens has released updates for the affected products, and recommends to update them to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINAMICS GH150: All versions	As only SIMATIC HMI image versions < V16 Update 4 are affected, please update the HMI Panel image as included in your installation of SINAMICS GH150 to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SINAMICS GL150 (with option X30): All versions	As only SIMATIC HMI image versions < V16 Update 4 are affected, please update the HMI Panel image as included in your installation of SINAMICS GL150 (with option X30) to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SINAMICS GM150 (with option X30): All versions	As only SIMATIC HMI image versions < V16 Update 4 are affected, please update the HMI Panel image as included in your installation of SINAMICS GM150 (with option X30) to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SINAMICS SH150: All versions	As only SIMATIC HMI image versions < V16 Update 4 are affected, please update the HMI Panel image as included in your installation of SINAMICS SH150 to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/

SINAMICS SL150: All versions	As only SIMATIC HMI image versions < V15 SP1 Update 6 are affected, please update the HMI Panel image as included in your installation of SINAMICS SL150 to V15 SP1 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890/
SINAMICS SM120: All versions	As only SIMATIC HMI image versions < V16 Update 4 are affected, please update the HMI Panel image as included in your installation of SINAMICS SM120 to V16 Update 4 or later version https://support.industry.siemens.com/cs/ww/en/view/109746530/
SINAMICS SM150: All versions	As only SIMATIC HMI image versions < V15 SP1 Update 6 are affected, please update the HMI Panel image as included in your installation of SINAMICS SM150 to V15 SP1 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890/
SINAMICS SM150i: All versions	As only SIMATIC HMI image versions < V15 SP1 Update 6 are affected, please update the HMI Panel image as included in your installation of SINAMICS SM150i to V15 SP1 Update 6 or later version https://support.industry.siemens.com/cs/ww/en/view/109763890/

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

- Disable Sm@rtServer in the SIMATIC HMI Comfort Panels system component of SINAMICS. If this is not possible, Defense-in-Depth should be used. Note: By default Sm@rtServer is disabled, but it can be enabled on request by the system integrator

- Follow SINAMICS MV Industrial Security guidelines

- For any questions regarding update, please contact Siemens customer service or your system integrator.

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

The SINAMICS medium voltage converter family is used to control a wide variety of medium voltage converters or inverters in different applications.

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

Vulnerability CVE-2021-27383

SmartVNC has a heap allocation leak vulnerability in the server Tight encoder, which could result in a Denial-of-Service condition.

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-770: Allocation of Resources Without Limits or Throttling

Vulnerability CVE-2021-27384

SmartVNC has an out-of-bounds memory access vulnerability in the device layout handler, represented by a binary data stream on client side, which can potentially result in code execution.

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-2021-27385

A remote attacker could send specially crafted packets to SmartVNC device layout handler on client side, which could influence the amount of resources consumed and result in a Denial-of-Service (infinite loop) condition.

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-400: Uncontrolled Resource Consumption

Vulnerability CVE-2021-27386

SmartVNC has a heap allocation leak vulnerability in the device layout handler on client side, which could result in a Denial-of-Service condition.

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-401: Missing Release of Memory after Effective Lifetime

ADDITIONAL INFORMATION

The CVSS score of the vulnerabilities listed in this advisory relate to the original affected HMI devices listed in SSA-538778 and SSA-940818. The CVSS score for the products listed in this advisory is CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:L/I:H/A:H/E:P/RL:O/RC:C (Base Score: 7.7).

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
V1.1 (2021-08-10):	Updated information for SINAMICS SL150, SINAMICS SM150 and SINAMICS SM150i

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.