SSA-538778: SmartVNC Vulnerabilities in SIMATIC HMI/WinCC Products

Publication Date: 2021-05-11
Last Update: 2021-10-12
Current Version: V1.2
CVSS v3.1 Base Score: 9.8

SUMMARY

Multiple SmartVNC vulnerabilities in the affected products listed below could allow remote code execution and Denial-of-Service attacks under certain conditions.

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

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Comfort Outdoor Panels V15 7" & 15" (incl. SIPLUS variants): All versions < V15.1 Update 6	Update SIMATIC WinCC (TIA Portal) to V15.1 Update 6, and then update panel to V15.1 Update 6 https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC HMI Comfort Outdoor Panels V16 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 V15 4" - 22" (incl. SIPLUS variants): All versions < V15.1 Update 6	Update SIMATIC WinCC (TIA Portal) to V15.1 Update 6, and then update panel to V15.1 Update 6 https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC HMI Comfort Panels V16 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 V15 KTP400F, KTP700, KTP700F, KTP900 and KTP900F: All versions < V15.1 Update 6	Update SIMATIC WinCC (TIA Portal) to V15.1 Update 6, and then update panel to V15.1 Update 6 https://support.industry.siemens.com/cs/ww/en/view/109763890/
SIMATIC HMI KTP Mobile Panels V16 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 V15: All versions < V15.1 Update 6	Update to V15.1 Update 6 https://support.industry.siemens.com/cs/ww/en/view/109763890/

SIMATIC WinCC Runtime Advanced V16: 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 HMI Panels are used for operator control and monitoring of machines and plants.

SIMATIC WinCC Runtime Advanced is a visualization runtime platform 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-2021-25660

SmartVNC has an out-of-bounds memory access vulnerability that could be triggered on the server side when sending data from the client, which could result in a Denial-of-Service condition.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:R/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-788: Access of Memory Location After End of Buffer

Vulnerability CVE-2021-25661

SmartVNC has an out-of-bounds memory access vulnerability that could be triggered on the client side when sending data from the server, which could result in a Denial-of-Service condition.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-788: Access of Memory Location After End of Buffer

Vulnerability CVE-2021-25662

SmartVNC client fails to handle an exception properly if the program execution process is modified after sending a packet from the server, which could result in a Denial-of-Service condition.

CVSS v3.1 Base Score	5.9
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:L/I:N/A:H/E:P/RL:O/RC:C
CWE	CWE-755: Improper Handling of Exceptional Conditions

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

- V15.1 Update 6 solution was added to support users that can´t update to V16 Update 4

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 (2021-09-14):   Added additional solution for all products
V1.2 (2021-10-12):   V15 sub-version numbering correction

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.