SSA-478893: TightVNC Vulnerabilities in Industrial Products

Publication Date: 2020-12-08
Last Update: 2020-12-08
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Multiple TightVNC (V1.x) vulnerabilities in the affected products could allow remote code execution and Denial-of-Service attacks under certain conditions.

Siemens has released updates for several affected products, is working on updates for the remaining affected products and recommends specific countermeasures until fixes are available.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIMATIC HMI Comfort Outdoor Panels 7" & 15" (incl. SIPLUS variants): All versions < V16 Update 3	Update SIMATIC WinCC (TIA Portal) to V16 Update 3 or newer, and then update panel to V16 Update 3 or newer https://support.industry.siemens.com/cs/ww/en/view/109775861
SIMATIC HMI Comfort Panels 4" - 22" (incl. SIPLUS variants): All versions < V16 Update 3	Update SIMATIC WinCC (TIA Portal) to V16 Update 3 or newer, and then update panel to V16 Update 3 or newer 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 3	Update SIMATIC WinCC (TIA Portal) to V16 Update 3 or newer, and then update panel to V16 Update 3 or newer https://support.industry.siemens.com/cs/ww/en/view/109775861
SIMATIC ITC1500 V3.1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC1500 V3.1 PRO: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC1900 V3.1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC1900 V3.1 PRO: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC2200 V3.1: All versions	See recommendations from section Workarounds and Mitigations
SIMATIC ITC2200 V3.1 PRO: All versions	See recommendations from section Workarounds and Mitigations

SIMATIC WinCC Runtime Advanced: All versions < V16 Update 3	Update to V16 Update 3 or newer https://support.industry.siemens.com/cs/ww/en/view/109776018
SIMATIC WinCC Runtime Professional: All versions < V16 Update 3	Update to V16 Update 3 or newer https://support.industry.siemens.com/cs/ww/en/view/109776017

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

SIMATIC ITC Industrial Thin Clients represent powerful control terminals with high-resolution wide-screen touch displays in 12, 15, 19 and 22 inch formats.

SIMATIC WinCC Runtime Advanced/Professional 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-2019-15678

TightVNC code version 1.3.10 contains heap buffer overflow in rfbServerCutText handler, which can potentially result in code execution. This attack appear to be exploitable via network connectivity.

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-2019-15679

TightVNC code version 1.3.10 contains heap buffer overflow in InitialiseRFBConnection function, which can potentially result in code execution. This attack appear to be exploitable via network connectivity.

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-2019-15680

TightVNC code version 1.3.10 contains null pointer dereference in HandleZlibBPP function, which could result in a Denial-of-Service (DoS). This attack appear to be exploitable via network connectivity.

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-476: NULL Pointer Dereference

Vulnerability CVE-2019-8287

TightVNC code version 1.3.10 contains global buffer overflow in HandleCoRREBBP macro function, which can potentially result in code execution. This attack appear to be exploitable via network connectivity.

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-120: Buffer Copy without Checking Size of Input (‘Classic Buffer Overflow’)

ADDITIONAL INFORMATION

Listed vulnerabilities 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 (2020-12-08): 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.