SSA-390195: LibVNC Vulnerabilities in SIMATIC ITC Products

Publication Date: 2021-12-14
Last Update: 2021-12-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.8

SUMMARY

Multiple LibVNC 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 ITC1500 V3: All versions < V3.2.1.0	Update to V3.2.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109804128/ See further recommendations from section Workarounds and Mitigations
SIMATIC ITC1500 V3 PRO: All versions < V3.2.1.0	Update to V3.2.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109804128/ See further recommendations from section Workarounds and Mitigations
SIMATIC ITC1900 V3: All versions < V3.2.1.0	Update to V3.2.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109804128/ See further recommendations from section Workarounds and Mitigations
SIMATIC ITC1900 V3 PRO: All versions < V3.2.1.0	Update to V3.2.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109804128/ See further recommendations from section Workarounds and Mitigations
SIMATIC ITC2200 V3: All versions < V3.2.1.0	Update to V3.2.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109804128/ See further recommendations from section Workarounds and Mitigations
SIMATIC ITC2200 V3 PRO: All versions < V3.2.1.0	Update to V3.2.1.0 or later version https://support.industry.siemens.com/cs/ww/en/view/109804128/ See further recommendations from section Workarounds and Mitigations

WORKAROUNDS AND MITIGATIONS

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

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

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-2017-18922

websockets.c in LibVNCServer prior to 0.9.12 did not properly decode certain WebSocket frames. A malicious attacker could exploit this by sending specially crafted WebSocket frames to a server, causing a heap-based buffer overflow.

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:U/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2018-20019

LibVNC before commit a83439b9fbe0f03c48eb94ed05729cb016f8b72f contains multiple heap out-of-bound write vulnerabilities in VNC client code that can result remote 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:U/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2018-20748

LibVNC before 0.9.12 contains multiple heap out-of-bounds write vulnerabilities in libvncclient/rfbproto.c. The fix for CVE-2018-20019 was incomplete.

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:U/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2018-20749

LibVNC before 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.

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:U/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2018-20750

LibVNC through 0.9.12 contains a heap out-of-bounds write vulnerability in libvncserver/rfbserver.c. The fix for CVE-2018-15127 was incomplete.

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:U/RL:O/RC:C
CWE	CWE-787: Out-of-bounds Write

Vulnerability CVE-2018-21247

An issue was discovered in LibVNCServer before 0.9.13. There is an information leak (of uninitialized memory contents) in the libvncclient/rfbproto.c ConnectToRFBRepeater function.

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:U/RL:O/RC:C
CWE	CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Vulnerability CVE-2019-15681

LibVNC commit before d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a contains a memory leak (CWE-655) in VNC server 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 appear to be exploitable via network connectivity. These vulnerabilities have been fixed in commit d01e1bb4246323ba6fcee3b82ef1faa9b1dac82a.

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

Vulnerability CVE-2019-15690

A flaw was found in libvncserver. An integer overflow within the HandleCursorShape() function can be exploited to cause a heap-based buffer overflow by tricking a user or application using libvncserver to connect to an unstrusted server and subsequently send cursor shapes with specially crafted dimensions. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.

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:U/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-20788

libvncclient/cursor.c in LibVNCServer through 0.9.12 has a HandleCursorShape integer overflow and heap-based buffer overflow via a large height or width value. NOTE: this may overlap CVE-2019-15690.

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:U/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2019-20839

libvncclient/sockets.c in LibVNCServer before 0.9.13 has a buffer overflow via a long socket filename.

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:U/RL:O/RC:C
CWE	CWE-120: Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')

Vulnerability CVE-2019-20840

An issue was discovered in LibVNCServer before 0.9.13. libvncserver/ws_decode.c can lead to a crash because of unaligned accesses in hybiReadAndDecode.

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:U/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2020-14396

An issue was discovered in LibVNCServer before 0.9.13. libvncclient/tls_openssl.c has a NULL pointer dereference.

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:U/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2020-14397

An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rfbregion.c has a NULL pointer dereference.

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:U/RL:O/RC:C
CWE	CWE-476: NULL Pointer Dereference

Vulnerability CVE-2020-14398

An issue was discovered in LibVNCServer before 0.9.13. An improperly closed TCP connection causes an infinite loop in libvncclient/sockets.c.

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:U/RL:O/RC:C
CWE	CWE-835: Loop with Unreachable Exit Condition (‘Infinite Loop’)

Vulnerability CVE-2020-14401

An issue was discovered in LibVNCServer before 0.9.13. libvncserver/scale.c has a pixel_value integer overflow.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:L/A:L/E:U/RL:O/RC:C
CWE	CWE-190: Integer Overflow or Wraparound

Vulnerability CVE-2020-14402

An issue was discovered in LibVNCServer before 0.9.13. libvncserver/corre.c allows out-of-bounds access via encodings.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L/E:U/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2020-14403

An issue was discovered in LibVNCServer before 0.9.13. libvncserver/hextile.c allows out-of-bounds access via encodings.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L/E:U/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2020-14404

An issue was discovered in LibVNCServer before 0.9.13. libvncserver/rre.c allows out-of-bounds access via encodings.

CVSS v3.1 Base Score	5.4
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:N/A:L/E:U/RL:O/RC:C
CWE	CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer

Vulnerability CVE-2020-14405

An issue was discovered in LibVNCServer before 0.9.13. libvncclient/rfbproto.c does not limit TextChat size.

CVSS v3.1 Base Score	6.5
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H/E:U/RL:O/RC:C
CWE	CWE-770: Allocation of Resources Without Limits or Throttling

ADDITIONAL INFORMATION

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 (2021-12-14): Publication Date

TERMS OF USE