SSA-170881: Vulnerabilities in SINUMERIK Controllers

Publication Date:	2018-12-11
Last Update:	2019-03-12
Current Version:	V1.1
CVSS v3.0 Base Score:	10.0

SUMMARY

The latest updates for SINUMERIK controllers fix multiple security vulnerabilities that could allow an attacker to cause Denial-of-Service conditions, escalate privileges, or to execute code from remote.

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. Siemens recommends to update affected devices as soon as possible.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SINUMERIK 808D V4.7: All versions < V4.91 only affected by CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11465, CVE-2018-11466	Update to V4.91 and follow recommendations from section Workarounds and Mitigations. SINUMERIK software can be obtained from your local Siemens account manager.
SINUMERIK 808D V4.8: All versions < V4.91 only affected by CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11462, CVE-2018-11463, CVE-2018-11465, CVE-2018-11466	Update to V4.91 and follow recommendations from section Workarounds and Mitigations. SINUMERIK software can be obtained from your local Siemens account manager.
SINUMERIK 828D V4.7: All versions < V4.7 SP6 HF1	Update to V4.7 SP6 HF1 and follow recommendations from section Workarounds and Mitigations. SINUMERIK software can be obtained from your local Siemens account manager.
SINUMERIK 840D sl V4.7: All versions < V4.7 SP6 HF5	Update to V4.7 SP6 HF5 and follow recommendations from section Workarounds and Mitigations. SINUMERIK software can be obtained from your local Siemens account manager.
SINUMERIK 840D sl V4.8: All versions < V4.8 SP3	Update to V4.8 SP3 and follow recommendations from section Workarounds and Mitigations. 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:

- Check and restore default settings (4842/tcp and 5900/tcp blocked) for firewall on port X130

- Restrict system access to authorized personnel and follow a least privilege approach
- Apply cell protection concept
- Use VPN for protecting network communication between cells
- Apply Defense-in-Depth

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 CNC offers automation solutions for the shop floor, job shops and large serial production environments.

VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

Vulnerability CVE-2018-11457

The integrated web server on port 4842/tcp of the affected products could allow a remote attacker to execute code with privileged permissions on the system by sending specially crafted network requests to port 4842/tcp.

Please note that this vulnerability is only exploitable if port 4842/tcp is manually opened in the firewall configuration of network port X130.

The security vulnerability could be exploited by an attacker with network access to the affected devices on port 4842/tcp. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the web server.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11458

The integrated VNC server on port 5900/tcp of the affected products could allow a remote attacker to execute code with privileged permissions on the system by sending specially crafted network requests to port 5900/tcp.

Please note that this vulnerability is only exploitable if port 5900/tcp is manually opened in the firewall configuration of network port X130.

The security vulnerability could be exploited by an attacker with network access to the affected devices and port. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the VNC server.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11459

A local attacker could modify a user-writeable configuration file so that after reboot or manual initiation the system reloads the modified configuration file and attacker-controlled code is executed with elevated privileges.

The security vulnerability could be exploited by an attacker with local access to the affected system. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.0
CVSS Vector	CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11460

A local attacker with elevated user privileges (manufact) could modify a CRAMFS archive so that after reboot the system loads the modified CRAMFS file and attacker-controlled code is executed with root privileges.

The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires elevated user privileges (manufact) but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	6.7
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:H/E:P/RL:T/RC:C

Vulnerability CVE-2018-11461

A local attacker with user privileges could use the service command application for privilege escalation to an elevated user but not root.

The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	6.6
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:L/I:H/A:L/E:P/RL:O/RC:C

Vulnerability CVE-2018-11462

By sending a specially crafted authentication request to the affected systems a remote attacker could escalate his privileges to an elevated user account but not to root.

The security vulnerability could be exploited by an attacker with network access to the affected systems. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	9.8
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11463

A buffer overflow in the service command application could allow a local attacker to execute code with elevated privileges.

The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.8
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11464

The integrated VNC server on port 5900/tcp of the affected products could allow a remote attacker to cause a Denial-of-Service condition of the VNC server.

Please note that this vulnerability is only exploitable if port 5900/tcp is manually opened in the firewall configuration of network port X130.

The security vulnerability could be exploited by an attacker with network access to the affected devices and port. Successful exploitation requires no privileges and no user interaction. The vulnerability could allow an attacker to compromise availability of the VNC server.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	5.3
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RL:O/RC:C

Vulnerability CVE-2018-11465

A local attacker could use ioctl calls to do out of bounds reads, arbitrary writes, or execute code in kernel mode.

The security vulnerability could be exploited by an attacker with local access to the affected systems. Successful exploitation requires user privileges but no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known.

CVSS v3.0 Base Score	7.8
CVSS Vector	CVSS:3.0/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C

Vulnerability CVE-2018-11466

Specially crafted network packets sent to port 102/tcp (ISO-TSAP) could allow a remote attacker to either cause a Denial-of-Service condition of the integrated software firewall or allow to execute code in the context of the software firewall.

The security vulnerability could be exploited by an attacker with network access to the affected systems on port 102/tcp. Successful exploitation requires no user privileges and no user interaction. The vulnerability could allow an attacker to compromise confidentiality, integrity and availability of the system.

At the time of advisory publication no public exploitation of this security vulnerability was known

CVSS v3.0 Base Score	10.0
CVSS Vector	CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Anton Kalinin, Danila Parnishchev, Dmitry Sklyar, Gleb Gritsai, Kirill Nesterov, Radu Motspan, and Sergey Sidorov from Kaspersky Lab for coordinated disclosure of vulnerabilities CVE-2018-11457, CVE-2018-11458, CVE-2018-11459, CVE-2018-11460, CVE-2018-11461, CVE-2018-11463, CVE-2018-11464, CVE-2018-11465, and CVE-2018-11466.

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 (2018-12-11):	Publication Date
V1.1 (2019-03-12):	Added update for SINUMERIK 808D

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.