SSA-632562: Vulnerabilities in SIPROTEC 5 Ethernet plug-in communication modules and devices

Publication Date:	2019-08-02
Last Update:	2020-01-14
Current Version:	V1.2
CVSS v3.1 Base Score:	9.8

SUMMARY

The SIPROTEC 5 Ethernet plug-in communication modules and devices are affected by multiple security vulnerabilities. These vulnerabilities could allow an attacker to leverage various attacks, e.g. to execute arbitrary code over the network.

The underlying Wind River VxWorks network stack is affected by eleven vulnerabilities known as 'URGENT/11'. Of these, two DHCP-related vulnerabilities (CVE-2019-12257 and CVE-2019-12264) do not apply to this advisory as the listed products use a different DHCP stack.

One further vulnerability affects the boot process of the device under certain conditions.

Siemens has released updates and recommends that customers update to the new versions.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
Ethernet plug-in communication modules for SIPROTEC 5 devices with CPU variants CP300 and CP100: All versions < V7.91 only affected by CVE-2019-12255, CVE-2019-12256, CVE-2019-12258, CVE-2019-12259, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12265	Update to communication protocols firmware version V7.91 or higher. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/us/en/view/109740816
Ethernet plug-in communication modules for SIPROTEC 5 devices with CPU variants CP200: All versions < V7.59 only affected by CVE-2019-12255, CVE-2019-12256, CVE-2019-12258, CVE-2019-12259, CVE-2019-12260, CVE-2019-12261, CVE-2019-12262, CVE-2019-12263, CVE-2019-12265	Update to communication protocols firmware version V7.59. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/document/109740816/siprotec-5-communication-protocols
SIPROTEC 5 devices with CPU variants CP300 and CP100: All versions < V8.01	Update to firmware version V8.01. Search for 'SIPROTEC 5 - DIGSI Device Drivers V8.01' on the Siemens Industry Online Support site. The firmware version V8.01 for the communication modules can also be found on each device-specific download page. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/ww/en/

SIPROTEC 5 devices with CPU variants CP200: All versions < V7.59 only affected by CVE-2019-10938	Update to firmware version V7.59. Search for 'SIPROTEC 5 - DIGSI Device Drivers V7.59' on the Siemens Industry Online Support site. The firmware version V7.59 for the communication modules can also be found on each device-specific download page. Applying the update causes the device / module to go through a single restart cycle. https://support.industry.siemens.com/cs/ww/en/

WORKAROUNDS AND MITIGATIONS

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

- Use a firewall to block traffic with "TCP Urgent Pointer" set to mitigate CVE-2019-12255, CVE-2019-12260, CVE-2019-12261, and CVE-2019-12263. See https://www.windriver.com/security/announcements/tcp-ip-network-stack-ipnet-urgent11/ for more information.
- Use a firewall to block traffic with IP-options SSRR (Strict Source and Record Route) or LSRR (Loose Source and Record Route) to mitigate CVE-2019-12256. See https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-12256 for more information.
- Use a firewall to block traffic with destination port 443/TCP or activate the role-based access control feature or the connection password feature in the device to mitigate CVE-2019-10938.
- To resolve CVE-2019-10938 for SIPROTEC 5 CP300 and CP100 CPU variant update to firmware version V7.90 or higher and update DIGSI 5 to V7.90 or higher from https://support.industry.siemens.com/cs/ww/en/ and activate the client authorization feature. Applying the update causes the device or module to go through a single restart cycle.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs) worldwide are usually required by regulations to build resilience into the power grids by applying multi-level redundant secondary protection schemes. It is therefore recommended that the operators check whether appropriate resilient protection measures are in place. The risk of cyber incidents impacting the grid's reliability can thus be minimized by virtue of the grid design.

Siemens strongly recommends applying the provided security updates using the corresponding tooling and documented procedures made available with the product. If supported by the product, an automated means to apply the security updates across multiple product instances may be used. Siemens strongly recommends prior validation of any security update before being applied, and supervision by trained staff of the update process in the target environment.

As a general security measure Siemens strongly recommends to protect network access with appropriate mechanisms (e.g. firewalls, segmentation, VPN). It is advised to configure the environment according to our operational guidelines in order to run the devices in a protected IT environment.

Recommended security guidelines to Secure Substations can be found at:

https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

SIPROTEC 5 devices provide a range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application.

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-2019-12255

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a device, an attacker could potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2019-12256

By sending IPv4 packets with specially crafted IP options to a device, an attacker could potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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-121: Stack-based Buffer Overflow

Vulnerability CVE-2019-12258

By sending TCP packets with specially crafted TCP options to a device, an attacker could potentially trigger a Denial-of-Service (DoS) condition. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2019-12259

By sending specially crafted IGMP packets to a device, an attacker could potentially trigger a Denial-of-Service (DoS) condition. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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-362: Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')

Vulnerability CVE-2019-12260

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a device, an attacker could potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

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-371: State Issues

Vulnerability CVE-2019-12261

While connecting to a remote host, specially crafted TCP packets with a manipulated TCP Urgent Pointer could potentially cause the execution of arbitrary code on the device. It is required that the affected device connects to a malicious system to conduct this attack.

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

CVSS v3.1 Base Score	8.8
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-191: Integer Underflow (Wrap or Wraparound)

Vulnerability CVE-2019-12262

By sending unsolicited reverse ARP packets to a device, an attacker may be able to affect availability and integrity of the device. Adjacent network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	7.1
CVSS Vector	CVSS:3.1/AV:A/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:L/E:P/RL:O/RC:C
CWE	CWE-840: Business Logic Errors

Vulnerability CVE-2019-12263

By sending specially crafted TCP packets with a manipulated TCP Urgent Pointer to a device, an attacker could potentially trigger a race condition and potentially execute arbitrary code. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	8.1
CVSS Vector	CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C
CWE	CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization (‘Race Condition’)

Vulnerability CVE-2019-12265

By sending specially crafted IGMPv3 packets to a device, an attacker may be able to obtain a limited amount of data from the device. Network access, but no authentication and no user interaction is needed to conduct this attack.

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

CVSS v3.1 Base Score	5.3
CVSS Vector	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C
CWE	CWE-840: Business Logic Errors

Vulnerability CVE-2019-10938

An unauthenticated attacker with network access to the device could potentially insert arbitrary code which is executed before firmware verification in the device.

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

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-284: Improper Access Control

ACKNOWLEDGMENTS

Siemens thanks the following parties for their efforts:

- Wind River for coordinated disclosure of CVE-2019-12255 - CVE-2019-12265
- Pierre Capillon, Nicolas Iooss, and Jean-Baptiste Galet from Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) for coordinated disclosure of CVE-2019-10938

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 (2019-08-02): Publication Date

V1.1 (2019-12-10): Added update for Ethernet plug-in communication modules for SIPROTEC 5 devices with CPU variants CP200

V1.2 (2020-01-14): Clarified affected products, added update for SIPROTEC 5 devices, removed DHCP vulnerablities as no products affected, updated summary for clarification

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.