SSA-617233: Urgent/11 TCP/IP Stack Vulnerabilities in SIPROTEC 4 7SJ66 Devices

Publication Date:	2023-11-14
Last Update:	2023-11-14
Current Version:	V1.0
CVSS v3.1 Base Score:	9.8

SUMMARY

SIPROTEC 4 7SJ66 devices are affected by multiple security vulnerabilities due to the underlying Wind River VxWorks network stack. This stack is affected by nine of the eleven vulnerabilities that are also known as “URGENT/11”.

The vulnerabilities could allow an attacker to execute a variety of exploits for the purpose of denial of service (DoS), data extraction, remote code execution, etc. targeting availability, integrity and confidentiality of the devices and data.

Siemens has released a new version for SIPROTEC 4 7SJ66 and recommends to update to the latest version.

AFFECTED PRODUCTS AND SOLUTION

Affected Product and Versions	Remediation
SIPROTEC 4 7SJ66: All versions < V4.41	Update to V4.41 or later version https://support.industry.siemens.com/cs/ww/en/view/109743555/

WORKAROUNDS AND MITIGATIONS

Product-specific remediations or mitigations can be found in the section Affected Products and Solution. Please follow the General Security Recommendations.

GENERAL SECURITY RECOMMENDATIONS

Operators of critical power systems (e.g. TSOs or DSOs) 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 can be found at: https://www.siemens.com/gridsecurity

PRODUCT DESCRIPTION

SIPROTEC 5 and SIPROTEC 4 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

Wind River VxWorks has a Buffer Overflow in the TCP component (issue 1 of 4). This is a IPNET security vulnerability: TCP Urgent Pointer = 0 that leads to an integer underflow.

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')

Vulnerability CVE-2019-12256

Wind River VxWorks 6.9 and vx7 has a Buffer Overflow in the IPv4 component. There is an IPNET security vulnerability: Stack overflow in the parsing of IPv4 packets' IP options.

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')

Vulnerability CVE-2019-12258

Wind River VxWorks 6.6 through vx7 has Session Fixation in the TCP component. This is a IPNET security vulnerability: DoS of TCP connection via malformed TCP options.

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-384: Session Fixation

Vulnerability CVE-2019-12259

Wind River VxWorks 6.6, 6.7, 6.8, 6.9 and vx7 has an array index error in the IGMPv3 client component. There is an IPNET security vulnerability: DoS via NULL dereference in IGMP parsing.

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-2019-12260

Wind River VxWorks 6.9 and vx7 has a Buffer Overflow in the TCP component (issue 2 of 4). This is an IPNET security vulnerability: TCP Urgent Pointer state confusion caused by a malformed TCP AO option.

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')

Vulnerability CVE-2019-12261

Wind River VxWorks 6.7 though 6.9 and vx7 has a Buffer Overflow in the TCP component (issue 3 of 4). This is an IPNET security vulnerability: TCP Urgent Pointer state confusion during connect() to a remote host.

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')

Vulnerability CVE-2019-12262

Wind River VxWorks 6.6, 6.7, 6.8, 6.9 and 7 has Incorrect Access Control in the RARP client component. IPNET security vulnerability: Handling of unsolicited Reverse ARP replies (Logical Flaw).

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-346: Origin Validation Error

Vulnerability CVE-2019-12263

Wind River VxWorks 6.9.4 and vx7 has a Buffer Overflow in the TCP component (issue 4 of 4). There is an IPNET security vulnerability: TCP Urgent Pointer state confusion due to race condition.

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

Wind River VxWorks 6.5, 6.6, 6.7, 6.8, 6.9.3 and 6.9.4 has a Memory Leak in the IGMPv3 client component. There is an IPNET security vulnerability: IGMP Information leak via IGMPv3 specific membership report.

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-401: Missing Release of Memory after Effective Lifetime

ADDITIONAL INFORMATION

For details regarding the individual URGENT/11 vulnerabilities see:

- Wind River advisories: https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2019-xxxxx
- NVD: https://nvd.nist.gov/vuln/detail/CVE-2019-xxxxx

(Replace `xxxxx` by the corresponding vulnerability id, e.g. by `12255`, or . . . , or `12265`)

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 (2023-11-14): 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.