**SSA-377115: SegmentSmack in Linux IP-Stack based Industrial Devices**

**SUMMARY**

The latest updates for the affected products fix a vulnerability that could allow remote attackers to affect the availability of the devices under certain conditions.

The underlying TCP stack can be forced to make very computation expensive calls for every incoming packet which can lead to a Denial-of-Service.

Siemens has released updates for some products, and is working on updates for the remaining affected products.

**AFFECTED PRODUCTS AND SOLUTION**

<table>
<thead>
<tr>
<th>Affected Product and Versions</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IE/PB-Link V3: All versions</td>
<td>See recommendations from section Workarounds and Mitigations</td>
</tr>
</tbody>
</table>
**WORKAROUNDS AND MITIGATIONS**

Siemens has not identified any specific mitigations or workarounds. Please follow General Security Recommendations.
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

IE/PB-Link devices enable existing PROFIBUS devices to be integrated into a PROFINET application.

RUGGEDCOM RM1224

ROX-based VPN endpoints and firewall devices are used to connect devices that operate in harsh environments such as electric utility substations and traffic control cabinets.

The SCALANCE M industrial routers are used for secure remote access to plants via mobile networks, e.g. GPRS or UMTS with the integrated security functions of a firewall for protection against unauthorized access and VPN to protect data transmission.

The SCALANCE S firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways.

The SCALANCE SC firewall is used to protect trusted industrial networks from untrusted networks. It allows filtering incoming and outgoing network connections in different ways.

SCALANCE W1700 products are wireless communication devices used to connect industrial components, like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs), according to the IEEE 802.11ac standard.

SCALANCE W700 products are wireless communication devices used to connect industrial components like Programmable Logic Controllers (PLCs) or Human Machine Interfaces (HMIs).

SIMATIC RF185C, RF186C and RF188C are communication modules for direct connection of SIMATIC identification systems to PROFINET IO/Ethernet and OPC UA

The SIMATIC CP 1243-1 communication processor connects the S7-1200 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1242-7 and CP 1243-7 LTE communication processors connect the S7-1200 controller to Wide Area Networks (WAN). It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

The SIMATIC CP 1243-8 IRC communication processor connects S7-1200 controllers via the SINAUT ST7 telecontrol protocol to a control center or master ST7 stations.

The SIMATIC CP 1543-1, CP 1543SP-1, CP 1542SP-1 and CP 1542SP-1 IRC communication processors connects the S7-1500 controller to Ethernet networks. It provides integrated security functions such as firewall, Virtual Private Networks (VPN) and support of other protocols with data encryption.

SINEMA Remote Connect ensures management of secure connections (VPN) between headquarters, service technicians and the installed machines or plants.

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-2018-5390

Linux kernel versions 4.9+ can be forced to make very expensive calls to tcp_collapse_ofo_queue() and
tcp_prune_ofo_queue() for every incoming packet which can lead to a denial of service.

<table>
<thead>
<tr>
<th>CVSS v3.1 Base Score</th>
<th>CVSS Vector</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-400: Uncontrolled Resource Consumption ('Resource Exhausion')</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Vulnerability CVE-2018-5391

The Linux kernel, versions 3.9+, is vulnerable to a denial of service attack with low rates of specially
modified packets targeting IP fragment re-assembly. An attacker may cause a denial of service
condition by sending specially crafted IP fragments. Various vulnerabilities in IP fragmentation
have been discovered and fixed over the years. The current vulnerability (CVE-2018-5391) became
exploitable in the Linux kernel with the increase of the IP fragment reassembly queue size.

<table>
<thead>
<tr>
<th>CVSS v3.1 Base Score</th>
<th>CVSS Vector</th>
<th>CWE</th>
</tr>
</thead>
<tbody>
<tr>
<td>CWE-20: Improper Input Validation</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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 (2020-04-14): 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.