# SSA-352504: Urgent/11 TCP/IP Stack Vulnerabilities in Siemens Power Meters

Publication Date: 2020-05-12
Last Update: 2020-06-09
Current Version: V1.1
CVSS v3.1 Base Score: 9.8

## SUMMARY

Siemens low & high voltage power meters are affected by multiple security vulnerabilities due to the underlying Wind River VxWorks network stack. This stack is affected by eleven vulnerabilities known as the “URGENT/11”.

The vulnerability could allow an attacker to execute a variety of exploits for the purpose of Denial-of-Service (DoS), data extraction, RCE, etc. targeting both availability and confidentiality of the devices and data.

Siemens is working on updates for the affected products, and recommends countermeasures until fixes are available.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| Siemens Power Meters Series 9410:<br>All versions < V2.2.1 | Update to firmware version V2.2.1<br>https://digitalcontentcenter.compas.siemens-info.com/9410_V002.002.001.zip |
| Siemens Power Meters Series 9810:<br>All versions | Update to firmware version V2.2.1<br>https://digitalcontentcenter.compas.siemens-info.com/9810_V002.002.001.zip |

## WORKAROUNDS AND MITIGATIONS

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

- Apply appropriate strategies for mitigation on the network level to ensure affected devices are as segmented.
- Apply Defense-in-Depth: https://www.siemens.com/cert/operational-guidelines-industrial-security

## 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

The Siemens 9410 series power and engery meters help meet the needs of your energy monitoring and cost management applications. These meters are ideally suited to local and remote monitoring of low or high-voltage electrical installations in industrial facilities, commercial buildings, utility networks or critical power environments.

The Siemens 9810 high accuracy and advanced power quality meter combines accurate; 3-phase energy and power measurement with data logging, power quality analysis, e-mail, alarming, Modbus mastering, Transient detection, Pre-Event/Post-Event Waveform capture and extensive I/O capablities in a highly flexible modular format.

## 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-2019-10938

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 |

### 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 |

## 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 (2020-05-12): Publication Date
V1.1 (2020-06-09): Update to include Siemens Power Meters Series 9810

## 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.