# SSA-359303: Debug Port in TIM 3V-IE and 4R-IE Family Devices

Publication Date: 2020-04-14
Last Update: 2020-04-14
Current Version: V1.0
CVSS v3.1 Base Score: 9.0

## SUMMARY

The latest update for TIM 3V-IE family devices and TIM 4R-IE family devices fixes a vulnerability that could allow an unauthenticated attacker with network access to port 17185/udp to gain full control over the device.

The devices are only vulnerable if the IP address is configured to 192.168.1.2.

Siemens has released updates for the affected products and recommends that customers update to the new version.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| TIM 3V-IE (incl. SIPLUS NET variants):<br>All versions < V2.8 | Update to V2.8<br>https://support.industry.siemens.com/cs/ww/en/view/109779003/ |
| TIM 3V-IE Advanced (incl. SIPLUS NET variants):<br>All versions < V2.8 | Update to V2.8<br>https://support.industry.siemens.com/cs/ww/en/view/109779003/ |
| TIM 3V-IE DNP3 (incl. SIPLUS NET variants):<br>All versions < V3.3 | Update to V3.3<br>https://support.industry.siemens.com/cs/ww/en/view/109779001/ |
| TIM 4R-IE (incl. SIPLUS NET variants):<br>All versions < V2.8 | Update to V2.8<br>https://support.industry.siemens.com/cs/ww/en/view/109779004/ |
| TIM 4R-IE DNP3 (incl. SIPLUS NET variants):<br>All versions < V3.3 | Update to V3.3<br>https://support.industry.siemens.com/cs/ww/en/view/109779002/ |

## WORKAROUNDS AND MITIGATIONS

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

- Set the IP of the device to anything other than 192.168.1.2.
- Limit access to port 17185/udp of an affected device (e.g. cell-protection firewall or corporate firewall) to reduce the risk.

## 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

TIM 3V-IE DNP3 communication module for SIMATIC S7-300 with an RS232 interface for DNP3 communication via a classic WAN and an RJ45 interface for DNP3 communication via a IP-based network (WAN or LAN)

TIM 3V-IE communication module for SIMATIC S7-300 with an RS232 interface for SINAUT communication via a classic WAN and an RJ45 interface for SINAUT communication via an IP-based network (WAN or LAN)

TIM 3V-IE advanced communication module for SIMATIC S7-300 with an RS232 interface for SINAUT communication via a classic WAN and an RJ45 interface for SINAUT communication via an IP-based network (WAN or LAN)

TIM 4R-IE communication module for SIMATIC S7-300, S7-400, PC; with two RS232/RS485 interfaces for SINAUT Communication via standard WAN and two RJ45 interfaces for SINAUT communication via IP-based networks (WAN or LAN)

TIM 4R-IE DNP3 communication module for SIMATIC S7-300, S7-400, PC; with two RS232/RS485 Interfaces for DNP3- Communication via standard WAN and two RJ45 interfaces for DNP3 communication via IP-based networks (WAN or LAN)

## 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-2019-10939

The affected versions contain an open debug port that is available under certain specific conditions. The vulnerability is only available if the IP address is configured to 192.168.1.2.

If available, the debug port could be exploited by an attacker with network access to the device. No user interaction is required to exploit this vulnerability. The vulnerability impacts confidentiality, integrity, and availability of the affected device.

At the stage of publishing this security advisory no public exploitation is known.

| | |
|---|---|
| CVSS v3.1 Base Score | 9.0 |
| CVSS Vector | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H/E:P/RL:O/RC:C |
| CWE | CWE-489: Active Debug Code |

## 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