# SSA-505225: Spectre Vulnerabilities in SIMATIC Industrial Thin Client V3

Publication Date: 2019-02-12
Last Update: 2019-02-12
Current Version: V1.0
CVSS v3.0 Base Score: 5.9

## SUMMARY

SIMATIC Industrial Thin Clients V3 contain a processor which is affected by vulnerabilities known under the name Spectre V1 and Spectre V4. Siemens has released updates for the affected products and recommends to update to the latest version.

## AFFECTED PRODUCTS AND SOLUTION

| Affected Product and Versions | Remediation |
|---|---|
| SIMATIC ITC1500 V3:<br>All versions < V3.1 | Update to V3.1<br>https://support.industry.siemens.com/cs/ww/en/view/109761864 |
| SIMATIC ITC1500 V3 PRO:<br>All versions < V3.1 | Update to V3.1<br>https://support.industry.siemens.com/cs/ww/en/view/109761864 |
| SIMATIC ITC1900 V3:<br>All versions < V3.1 | Update to V3.1<br>https://support.industry.siemens.com/cs/ww/en/view/109761864 |
| SIMATIC ITC1900 V3 PRO:<br>All versions < V3.1 | Update to V3.1<br>https://support.industry.siemens.com/cs/ww/en/view/109761864 |
| SIMATIC ITC2200 V3:<br>All versions < V3.1 | Update to V3.1<br>https://support.industry.siemens.com/cs/ww/en/view/109761864 |
| SIMATIC ITC2200 V3 PRO:<br>All versions < V3.1 | Update to V3.1<br>https://support.industry.siemens.com/cs/ww/en/view/109761864 |

## WORKAROUNDS AND MITIGATIONS

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

- As a prerequisite for an attack, an attacker must be able to run malicious code on affected systems. Therefore, Siemens recommends determining if it is possible that untrusted code can be run on these systems, or if existing measures implemented by the operator reduce the likelihood of untrusted code being run. Siemens recommends limiting the possibilities to run untrusted code if possible.
- SIMATIC Industrial Thin Clients V3 do not allow to install and run custom applications via its management interfaces. However, SIMATIC Industrial Thin Clients V3 could potentially allow to run

untrusted code via the web browser. Siemens recommends to only access trusted web sites using the built-in browser to further 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

SIMATIC ITC Industrial Thin Clients represent powerful control terminals with high-resolution wide-screen touch displays in 12, 15, 19 and 22 inch formats.

## VULNERABILITY CLASSIFICATION

The vulnerability classification has been performed by using the CVSS scoring system in version 3.0 (CVSS v3.0) (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.

### Vulnerability CVE-2017-5753

An attacker with local access to the system could potentially disclose information from protected memory areas via a side-channel attack on the processor cache.

| | |
|---|---|
| CVSS v3.0 Base Score | 5.9 |
| CVSS Vector | CVSS:3.0/AV:L/AC:H/PR:N/UI:N/S:C/C:H/I:N/A:N/E:P/RL:O/RC:C |

### Vulnerability CVE-2018-3639

An attacker with local access to the system could potentially disclose information from protected memory areas via a side-channel attack on the processor cache.

| | |
|---|---|
| CVSS v3.0 Base Score | 4.3 |
| CVSS Vector | CVSS:3.0/AV:L/AC:L/PR:N/UI:N/S:C/C:L/I:N/A:N/E:P/RL:O/RC:C |

## 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 (2019-02-12): 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.