America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Archived Content

In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.

ICS ADVISORY

Siemens S7-300/400 PLC Vulnerabilities (Update E)

Last Revised: March 10, 2020 **Alert Code:** ICSA-16-348-05

1. EXECUTIVE SUMMARY

- **CVSS v3 7.5**
- **ATTENTION:** Exploitable remotely/low skill level to exploit
- **Vendor:** Siemens
- **Equipment:** SIMATIC S7-300 and SIMATIC S7-400
- **Vulnerabilities:** Information Exposure, Improper Input Validation

2. UPDATE INFORMATION

This updated advisory is a follow-up to the advisory update titled ICSA-16-348-05 SIEMENS S7-300/400 PLC Vulnerabilities (Update D) that was published January 25, 2018, to the ICS webpage on us-cert.gov.

3. RISK EVALUATION

Successful exploitation of these vulnerabilities could lead to a denial-of-service condition or result in credential disclosure.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

The following products are affected:

--------- Begin Update E Part 1 of 1 ---------

- SIMATIC S7-300 CPU family (incl. related ET200 CPUs and SIPLUS variants) all versions
- SIMATIC S7-400 PN/DP V6 and below CPU family (incl. SIPLUS variants) all versions
- SIMATIC S7-400 PN/DP V7 CPU family (incl. SIPLUS variants) all versions
- SIMATIC S7-410 V8 CPU family (incl. SIPLUS variants) all versions (only affected by CVE-2016-9159)

4.2 VULNERABILITY OVERVIEW

4.2.1 INFORMATION EXPOSURE CWE-200

<https://cwe.mitre.org/data/definitions/200.html>

An attacker with network access to Port 102/TCP (ISO-TSAP) or via Profibus could obtain credentials from the PLC if Protection-Level 2 is configured on the affected devices.

CVE-2016-9159 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:n/a:n>).

4.2.2 IMPROPER INPUT VALIDATION CWE-20

<https://cwe.mitre.org/data/definitions/20.html>

Specially crafted packets sent to Port 80/TCP could cause the affected devices to go into defect mode. A cold restart is required to recover the system.

CVE-2016-9158 has been assigned to this vulnerability. A CVSS v3 base score of 7.5 has been assigned; the CVSS vector string is (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N <https://www.first.org/cvss/calculator/3.0#cvss:3.0/av:n/ac:l/pr:n/ui:n/s:u/c:h/i:n/a:n>).

--------- End Update E Part 1 of 1 ---------

4.3 BACKGROUND

- **CRITICAL INFRASTRUCTURE SECTORS:** Chemical, Energy, Food and Agriculture, and Water and Wastewater Systems
- **COUNTRIES/AREAS DEPLOYED:** Worldwide
- **COMPANY HEADQUARTERS LOCATION:** Germany

4.4 RESEARCHER

Zhu WenZhe from Beijing Acorn Network Technology reported these vulnerabilities to CISA.

5. MITIGATIONS

Siemens provides the following firmware versions to resolve CVE-2016-9158:

- SIMATIC S7-300 CPU family: Update to v3.X.14 <https://support.industry.siemens.com/cs/ww/en/ps/13752/dl>

- SIMATIC S7-400 PN v6: Update to v6.0.6 <https://support.industry.siemens.com/cs/de/en/view/109474874>
- SIMATIC S7-400 v7 CPU family: Update to v7.0.2 <https://support.industry.siemens.com/cs/ww/en/view/109752685>
- SIMATIC S7-410 v8 CPU family: Update to v8.2 <https://support.industry.siemens.com/cs/ww/en/view/109476571>

Siemens also recommends the following mitigations:

- Deactivate the web server.
- Apply Protection-Level 3 read/write protection.
- Apply cell protection concept.
- Apply defense-in-depth strategies.
- Use VPN for protecting network communication between cells.
- For SIMATIC S7-CPU 410 CPUs: Activate Field Interface Security in PCS 7 V9.0 and use a CP 443-1 Adv. to communicate with ES/OS in order to mitigate vulnerability 2 (CVE-2016-9159).

Siemens strongly recommends users protect network access with appropriate mechanisms (e.g., firewalls, segmentation, VPN). Siemens also advises that users configure the operational environment according to Siemens' Operational Guidelines for Industrial Security <https://www.siemens.com/cert/operational-guidelines-industrial-security>.

For more information on these vulnerabilities and more detailed mitigation instructions, please see Siemens Security Advisory SSA-731239 <http://www.siemens.com/cert/advisories>.

CISA recommends users take defensive measures to minimize the risk of exploitation of this vulnerability. Specifically, users should:

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet <https://www.us-cert.gov/ics/alerts/ics-alert-10-301-01>.

- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs), recognizing that VPNs may have vulnerabilities and should be updated to the most current version available. Also recognize that VPN is only as secure as the connected devices.

CISA reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

CISA also provides a section for control systems security recommended practices <https://www.us-cert.gov/ics/recommended-practices> on the ICS webpage on us-cert.gov <https://www.us-cert.gov/ics>. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies <https://www.us-cert.gov/sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf>.

Additional mitigation guidance and recommended practices are publicly available on the ICS webpage on us-cert.gov <https://www.us-cert.gov/ics> in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies <https://www.us-cert.gov/ics/tips/ics-tip-12-146-01b>.

Organizations observing any suspected malicious activity should follow their established internal procedures and report their findings to CISA for tracking and correlation against other incidents.

No known public exploits specifically target these vulnerabilities.

Vendor

- Siemens

Please share your thoughts

We recently updated our anonymous product survey; we welcome your feedback.

Return to top

Topics </topics> **Spotlight** </spotlight> **Resources & Tools** </resources-tools>

News & Events </news-events> **Careers** </careers> **About** </about>

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA Central

1-844-Say-CISA contact@cisa.dhs.gov

CISA.gov