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In an effort to keep CISA.gov current, the archive contains outdated information that may not reflect current policy or programs.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 SIMATIC S7-300 CPU Denial-of-Service Vulnerability

Last Revised: August 22, 2018 **Alert Code:** ICSA-15-064-04

OVERVIEW

Johannes Klick, Christian Pfahl, Martin Gebert, and Lucas Jacob from Freie Universität Berlin's work team SCADACS have identified a Denial-of-Service (DoS) vulnerability in Siemens SIMATIC S7-300 CPUs. Siemens has developed mitigations for this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

The following SIMATIC S7-300 CPUs are affected:

- SIMATIC S7-300 CPU family: all versions.

IMPACT

This vulnerability could allow attackers to perform a DoS attack over the network without prior authentication against S7-300 CPUs under certain conditions. A cold restart is required to recover the system.

Impact to individual organizations depends on many factors that are unique to each organization. NCCIC/ICS-CERT recommends that organizations evaluate the impact of this vulnerability based on their operational environment, architecture, and product implementation.

BACKGROUND

Siemens is a multinational company headquartered in Munich, Germany.

The affected product, SIMATIC S7-300 CPU, have been designed for process control in industrial environments. This product is deployed across several sectors including Chemical, Energy, Food and Agriculture, and Water and Wastewater Systems. Siemens estimates that these products are used primarily in the United States and Europe with a small percentage in Asia.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DENIAL-OF-SERVICE ATTACKCWE-404: Improper Resource Shutdown or Release, http://cwe.mitre.org/data/definitions/404, web site last accessed March 05, 2015.

Specially crafted packets sent to Port 102/TCP (ISO-TSAP) or via Profibus could cause the affected device to go into defect mode. A cold restart is required to recover the system.

CVE-2015-2177NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-2177, NIST uses this advisory to create the CVE web site report. This web site will be active sometime after publication of this advisory. has been assigned to this vulnerability. A CVSS v2 base score of 7.8 has been assigned; the CVSS vector string is (AV:N/AC:L/Au:N/C:N/I:N/A:C).CVSS Calculator, http://nvd.nist.gov/cvss.cfm?version=2&vector=AV:N/AC:L/Au:N/C:N/I:N/A:C, web site last accessed March 05, 2015.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

Crafting a working exploit for this vulnerability would be difficult.

MITIGATION

Siemens recommends the following mitigations:

- Apply protection-level 3 (Read/Write protection),
- Apply cell protection concept,Operational Guidelines for Industrial Security, https://www.siemens.com/cert/operational-guidelines-industrial-security, web site last accessed March 05, 2015.
- Use VPN for protecting network communication between cells, and
- Apply Defense-in-Depth.Further information about Defense-in-Depth, http://www.industry.siemens.com/topics/global/en/industrial-security/concept/Pages/defense-in-depth.aspx, web site last accessed March 05, 2015.

For more information on these vulnerabilities and detailed instructions, please see Siemens Security Advisory SSA-987029 at the following location:

http://www.siemens.com/cert/advisories <https://www.siemens.com/cert/advisories>

ICS-CERT encourages asset owners to take additional defensive measures to protect against this and other cybersecurity risks.

- Minimize network exposure for all control system devices and/or systems, and ensure that they are not accessible from the Internet.
- Locate control system networks and remote devices behind firewalls, and isolate them from the business network.

ICS-CERT also provides a section for control systems security recommended practices on the ICS-CERT web page at: http://ics-cert.us-cert.gov/content/recommended-practices </ics/content/recommended-practices>. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies. </sites/default/files/recommended_practices/nccic_ics-cert_defense_in_depth_2016_s508c.pdf> ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

Additional mitigation guidance and recommended practices are publicly available in the ICS-CERT Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies </ics/tips/ics-tip-12-146-01b>, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/ </ics/>).

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

In addition, ICS-CERT recommends that users take the following measures to protect themselves from social engineering attacks:

1. Do not click web links or open unsolicited attachments in email messages.
2. Refer to Recognizing and Avoiding Email ScamsRecognizing and Avoiding Email Scams, http://www.us-cert.gov/reading_room/emailscams_0905.pdf, web site last accessed March 05, 2015. for more information on avoiding email scams.
3. Refer to Avoiding Social Engineering and Phishing AttacksNational Cyber Alert System Cyber Security Tip ST04-014, http://www.us-cert.gov/cas/tips/ST04-014.html, web site last accessed March 05, 2015. for more information on social engineering attacks.

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