Siemens SIPROTEC Denial-of-Service Vulnerability | CISA

Published: 2018-08-27 · Archived: 2026-04-05 17:00:23 UTC

OVERVIEW

Siemens has identified a denial-of-service vulnerability in the SIPROTEC 4 and SIPROTEC Compact devices. This vulnerability was reported directly to Siemens by Victor Nikitin from i-Grids LLC Russia. Siemens has produced a new firmware update to mitigate this vulnerability.

This vulnerability could be exploited remotely.

AFFECTED PRODUCTS

Siemens reports that the vulnerability affects the following versions:

- SIPROTEC 4 and SIPROTEC Compact product families
- All devices that include the EN100 Ethernet module version V4.24 or prior.

IMPACT

An attacker could remotely cause a denial of service by exploiting this vulnerability.

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 products, SIPROTEC 4 and SIPROTEC Compact devices, provide a wide range of integrated protection, control, measurement, and automation functions for electrical substations and other fields of application. The EN100 module is used for enabling IEC 61850 communications with electrical/optical 100 Mbit interface for SIPROTEC 4 and SIPROTEC Compact devices. According to Siemens, SIPROTEC devices are deployed across several sectors including Energy. Siemens estimates that these products are used worldwide.

VULNERABILITY CHARACTERIZATION

VULNERABILITY OVERVIEW

DENIAL OF SERVICECWE-400: Uncontrolled Resource Consumption ('Resource Exhaustion'), http://cwe.mitre.org/data/definitions/400.html, web site last accessed July 21, 2015.

Specially crafted packets sent to Port 50000/UDP could cause a denial of service of the affected device. A manual reboot is required to return the device to service.

CVE-2015-5374NVD, http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-5374, 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 July 21, 2015.

VULNERABILITY DETAILS

EXPLOITABILITY

This vulnerability could be exploited remotely.

EXISTENCE OF EXPLOIT

No known public exploits specifically target this vulnerability.

DIFFICULTY

An attacker with a low skill would be able to exploit this vulnerability.

MITIGATION

Siemens has provided firmware update V4.25 for the EN100 module to fix the vulnerability.

The firmware update for SIPROTEC 4 can be obtained here:

http://www.siemens.com/downloads/siprotec-4

The firmware update for SIPROTEC Compact can be obtained here:

http://www.siemens.com/downloads/siprotec-compact

For more information on this vulnerability and more detailed mitigation instructions, please see Siemens Security Advisory SSA-732541 at the following location:

http://www.siemens.com/cert/advisories

ICS-CERT recommends that users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Configure firewall rules to appropriately restrict traffic to affected devices on Port 50000/UDP.
- Monitor traffic to affected devices on Port 50000/UDP with an intrusion detection system (IDS).
- 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.
- 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.

ICS-CERT reminds organizations to perform proper impact analysis and risk assessment prior to deploying defensive measures.

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. Several recommended practices are available for reading and download, including Improving Industrial Control Systems Cybersecurity with Defense-in-Depth Strategies.

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, that is available for download from the ICS-CERT web site (http://ics-cert.us-cert.gov/).

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.

Source: https://ics-cert.us-cert.gov/advisories/ICSA-15-202-01