مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity Vulnerability in Siemens Interniche IP-Stack

Tracking #:432318178

Date:25-12-2025

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that Siemens has disclosed a high-severity security vulnerability affecting multiple industrial products using the Interniche IP-Stack. The issue could allow an unauthenticated remote attacker to disrupt TCP connection establishment under certain conditions, potentially resulting in a denial-of-service (DoS) condition.

TECHNICAL DETAILS:

Vulnerability Details

- **CVE-2025-40820**
- **Severity:** CVSS v3.1: 8.7 High
- Affected products do not properly enforce TCP sequence number validation in certain scenarios and accept sequence numbers within a broad range. An unauthenticated remote attacker who is able to inject precisely timed TCP packets with spoofed source addresses could interfere with the TCP connection setup process. This may lead to a denial-of-service condition affecting TCP-based services.

Impact

- Denial of Service (DoS): Attackers could disrupt normal TCP connections to affected devices, potentially interrupting industrial operations.
- Operational Risk: Devices may become unresponsive, impacting critical manufacturing and OT environments.

Affected Products

The vulnerability affects a wide range of Siemens industrial automation and control products that incorporate the Interniche IP-Stack, including but not limited to:

- SIMATIC S7-1200, S7-1500, S7-300, S7-400 CPU families
- SIMATIC ET 200, ET 200SP, ET 200eco, ET 200pro modules
- SIMOCODE pro (PROFINET and Ethernet/IP variants)
- SINUMERIK 840D sl
- SIMATIC S7-200 SMART series
- SIPLUS industrial variants of the above products
- SIWAREX weighing systems

(Refer to the Siemens ProductCERT advisory for the complete and detailed list of affected models.)

Fixed Versions

Fixed versions vary by product line, including but not limited to:

- V1.3 or later
- V2.0.0 or later
- V4.4.0 or later
- V6.0.0 or later
- V8.3 or later
- V10.2 or later

RECOMMENDATIONS:

- Update affected devices to the latest Siemens firmware.

- If fixes aren't available: restrict TCP access to trusted IPs and disable unused Ethernet ports.
- Minimize device exposure and avoid direct internet connectivity.
- Use network segmentation and firewalls between OT and IT networks.
- Monitor network traffic for abnormal TCP connections.
- Follow Siemens guidance for additional product-specific mitigations if updates are pending.

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nvd.nist.gov/vuln/detail/CVE-2025-40820
- https://www.cisa.gov/news-events/ics-advisories/icsa-25-352-05