مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

High-Severity vulnerability in Siemens Products

Tracking #:432316303

Date:18-09-2024

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed a high-severity vulnerability in Siemens SIMATIC S7-200 SMART devices that could be exploited to remotely crash the device, causing a denial-of-service (DoS) condition.

TECHNICAL DETAILS:

A vulnerability (CVE-2024-43647) affecting Siemens SIMATIC S7-200 SMART devices. An unauthenticated remote attacker can exploit this vulnerability to cause a Denial-of-Service (DoS) condition, rendering the device unresponsive. Currently, there are no patches available for this vulnerability.

Vulnerability Details:

- **CVE-2024-43647**
- **CVSS v4.0** Base Score 8.7 High
- A vulnerability exists in SIMATIC S7-200 SMART devices that could allow an attacker to remotely cause a denial of service (DoS) condition by sending a specially crafted TCP packet.
- Successful exploitation of this vulnerability can lead to a complete denial-of-service affecting critical industrial processes controlled by the SIMATIC S7-200 SMART devices.

Affected Versions:

- SIMATIC S7-200 SMART CPU CR40 (6ES7288-1CR40-0AA0): All versions
- SIMATIC S7-200 SMART CPU CR60 (6ES7288-1CR60-0AA0): All Versions
- SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA0): All Versions
- SIMATIC S7-200 SMART CPU SR20 (6ES7288-1SR20-0AA1): All Versions
- SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA0): All Versions
- SIMATIC S7-200 SMART CPU SR30 (6ES7288-1SR30-0AA1): All Versions
- SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA0): All Versions
- SIMATIC S7-200 SMART CPU SR40 (6ES7288-1SR40-0AA1): All Versions
- SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA0): All Versions
- SIMATIC S7-200 SMART CPU SR60 (6ES7288-1SR60-0AA1): All Versions
- SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA0): All Versions
- SIMATIC S7-200 SMART CPU ST20 (6ES7288-1ST20-0AA1): All Versions
- SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA0): All Versions
- SIMATIC S7-200 SMART CPU ST30 (6ES7288-1ST30-0AA1): All Versions
- SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA0): All Versions
- SIMATIC S7-200 SMART CPU ST40 (6ES7288-1ST40-0AA1): All Versions
- SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA0): All Versions
- SIMATIC S7-200 SMART CPU ST60 (6ES7288-1ST60-0AA1): All Versions

Workarounds and Mitigations:

- **Limit Network Access:** Restrict network access to the affected devices only to trusted users and systems. Implement network segmentation to isolate these devices from critical systems and the internet.

RECOMMENDATIONS:

The UAE Cyber Security Council recommends applying the mitigation or workaround provided by Siemens.

- **Patching (When Available):** Apply any future patches released by Siemens to address this vulnerability.

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://cert-portal.siemens.com/productcert/html/ssa-969738.html?ste_sid=a6beb3257a28c5a5721ebac6f5e1d935