Schneider Electric Triconex Tricon (Update B) | CISA

Published: 2018-12-18 · Archived: 2026-04-05 16:58:28 UTC

1. EXECUTIVE SUMMARY

- **CVSS v3 9.0**

- **ATTENTION**: Exploitable remotely/HatMan malware specifically targets these vulnerabilities.
- **Vendor**: Schneider Electric
- **Equipment**: Triconex Tricon, Model 3008
- **Vulnerabilities**: Improper Restriction of Operations within the Bounds of a Memory Buffer

2. UPDATE INFORMATION

This updated advisory is a follow-up to the updated advisory titled ICSA-18-107-02 Schneider Electric Triconex Tricon (Update A) that was published May 3, 2018, on the NCCIC/ICS-CERT website.

3. RISK EVALUATION

Successful exploitation of these vulnerabilities could misinform or control the safety instrumented system which could result in arbitrary code execution, system shutdown, or the compromise of safety systems.

4. TECHNICAL DETAILS

4.1 AFFECTED PRODUCTS

The following versions of Triconex Tricon, a Safety Instrumented System, are affected:

- MP Model 3008 firmware versions 10.0-10.4

4.2 VULNERABILITY OVERVIEW

4.2.1 IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER CWE-119

System calls read directly from memory addresses within the control program area without any verification. Manipulating this data could allow attacker data to be copied anywhere within memory.

CVE-2018-8872 has been assigned to this vulnerability. A CVSS v3 base score of 9.0 has been calculated; the CVSS vector string is (AV:N/AC:H/PR:N/UI:N/S:C/C:H/I:H/A:H).

4.2.2 IMPROPER RESTRICTION OF OPERATIONS WITHIN THE BOUNDS OF A MEMORY BUFFER CWE-119

When a system call is made, registers are stored to a fixed memory location. Modifying the data in this location could allow attackers to gain supervisor-level access and control system states.

CVE-2018-7522 has been assigned to this vulnerability. A CVSS v3 base score of 7.9 has been assigned; the CVSS vector string is (AV:L/AC:L/PR:H/UI:N/S:C/C:N/I:H/A:H).

4.3 BACKGROUND

- **Critical Infrastructure Sectors:** Multiple Sectors
- **Countries/Areas Deployed:** Worldwide
- **Company Headquarters Location:** France

4.4 RESEARCHER

These vulnerabilities were discovered by NCCIC and Schneider Electric during the investigation of the HatMan malware.

5. MITIGATIONS

--------- Begin Update B Part 1 of 1 --------

5.1 VENDOR RECOMMENDATION

Schneider Electric has released the following security notification:

https://www.schneider-electric.com/en/download/document/SEVD-2017-347-01/

Schneider Electric strongly recommends that users upgrade to the latest Triconex Tricon CX version. Tricon CX v11.4 is now available and is compliant with the IEC 62443 cybersecurity standard and includes multiple security enhancements that meet the challenges posed by HatMan malware techniques and other sophisticated methods of attack. To upgrade your system, contact your field site support representative or contact Schneider Electric support.

5.1.1 DETECT AND RESPOND

Triconex users should contact their local Schneider Electric office for assistance. With this engagement, Schneider Electric will gather data from each Tricon safety system installation, analyze for the presence of the malware, and carry out any necessary malware removal procedures.

For users who choose to gather data from each Tricon safety system installation on their own, instructions and support material is available for download via the Schneider Electric Process Automation customer support portal (login required). The data will still need to be sent to Schneider Electric for analysis. As of February 1, 2019, Schneider Electric will require customers to have a support contract in place to engage with the HatMan malware detection service.

--------- End Update B Part 1 of 1 --------

Once Schneider Electric has analyzed this data, Triconex users will receive a report for each Tricon system analyzed. This report will advise whether the malware was detected, and what the next steps are to remove the malware if detected.

A YARA rule that matches the binary components of the HatMan malware is available for download at https://ics-cert.us-cert.gov/sites/default/files/file_attach/MAR-17-352-01.yara or by contacting Schneider Electric Customer Support.

5.1.2 DEFEND

The HatMan malware requires unrestricted access to the safety network via remote network or physical access. Additionally, the malware requires the Tricon key switch to be in the "PROGRAM" mode to successfully deploy its payload.

Schneider Electric continues to recommend users always implement the instructions in the "Security Considerations" section in the standard Triconex documentation (i.e., Planning and Installation Guides and TriStation 1131 Developers Guide), which include the following:

- Ensure the cybersecurity features in Triconex solutions are always enabled.
- Safety systems must always be deployed on isolated networks.
- Physical controls should be in place so that no unauthorized person would have access to the safety controllers, peripheral safety equipment, or the safety network.
- All controllers should reside in locked cabinets and never be left in the "PROGRAM" mode.
- All TriStation engineering workstations should be secured and never be connected to any network other than the safety network.
- All methods of mobile data exchange with the isolated safety network such as CDs, USB drives, DVD's, etc. should be scanned before use in the TriStation engineering workstations or any node connected to this network.
- Laptops and PCs should always be properly verified to be virus and malware free before connecting to the safety network or any Triconex controller.
- Operator stations should be configured to display an alarm whenever the Tricon key switch is in the "PROGRAM" mode.

5.2 NCCIC Recommendations

NCCIC recommends users take defensive measures to minimize the risk of exploitation of these vulnerabilities. Specifically, users should:

- Minimize network exposure for all Safety Instrumented Systems, and ensure that they are not accessible from the Internet.
- Locate Safety Instrumented Systems behind firewalls, and isolate them from all other networks.
- 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.

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

NCCIC also provides a section for control systems security recommended practices on the ICS-CERT web page. 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 on the ICS-CERT website in the Technical Information Paper, ICS-TIP-12-146-01B--Targeted Cyber Intrusion Detection and Mitigation Strategies.

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

NCCIC also recommends that users take the following measures to protect themselves from social engineering attacks:

- Do not click web links or open unsolicited attachments in email messages.
- Refer to Recognizing and Avoiding Email Scams for more information on avoiding email scams.
- Refer to Avoiding Social Engineering and Phishing Attacks for more information on social engineering attacks.

HatMan malware specifically targets these vulnerabilities. These vulnerabilities are exploitable remotely. High skill level is needed to exploit.
