Security Notification – ConneXium Lite Managed Switch

4-Feb-2016

Overview

Schneider Electric has become aware of a vulnerability in the ConneXium Lite managed Switch product.

Vulnerability Overview

The vulnerability identified may allow unauthorized upload of firmware.

Product(s) Affected

The product affected:

- ConneXium Lite Managed Switch, TCSESL043F23F0, and versions 01.01 and all previous versions

Vulnerability Details

The unauthorized firmware upload allows attackers, who are able to reach the management interface (the HTTP server) of the device to bypass authentication for a firmware upload. A further step of customizing a firmware image to include malicious code is necessary to exploit this weakness. The work required to achieve this is comprised of reverse-engineering as well as deep system knowledge.

Affected devices are vulnerable to switch to different software versions further widening the attack surface. A downgrade could also possibly cause a Denial-of-Service in network topologies not fully supported by older versions. With considerable effort, an attacker could insert malicious code into the device and gain control of its operation and modify the traffic going through it.

Overall CVSS Score: 5.0
(AV:N/AC:L/Au:N/C:P/I:C/A:N/E:F/RL:OF/RC:C/CDP:ND/TD:ND/CR:L/IR:L/AR:L)

Mitigation

A firmware with the fix for this vulnerability is available for download.

http://www.schneider-electric.com/download/ww/en/details/1727425936-TCSESL043F23F0_ConneXium-firmware_V0102

The following workaround can also be implemented to prevent this system flaw from being exploited. Schneider Electric recommends shielding the TCSESL043F23F0 web interface from public access. The device should only be connected to an intranet and the management interface not exposed to the public. If necessary, the device should be placed behind a firewall that implements this kind of restriction.

For More Information

This document is intended to help provide an overview of the identified vulnerability and actions required to mitigate it. To obtain full details on the issues and assistance on how to protect your installation, please contact your local Schneider Electric representative. These organizations will be fully aware of the situation and can support you through the process.

For further information on vulnerabilities in Schneider Electric's products, please visit Schneider Electric's cybersecurity web page at http://www2.schneider-electric.com/sites/corporate/en/support/cybersecurity/cybersecurity.page

About Schneider Electric

As a global specialist in energy management with operations in more than 100 countries, Schneider Electric offers integrated solutions across multiple market segments, including leadership positions in Utilities & Infrastructures, Industries & Machine Manufacturers, Non-residential Buildings, Data Centers & Networks and in Residential.
www.schneider-electric.com