Schneider Electric Security Notification

ConneXium Tofino Firewall and Loadable Security Modules

11 January 2022

Overview

Schneider Electric is aware of multiple vulnerabilities in its ConneXium Tofino Firewall products, and associated Loadable Security Modules (LSM)

Connexium Tofino Firewall and LSM products are part of the ConneXium Tofino Industrial Security Solution providing package for securing industrial control systems, particularly at the Local Area Network (LAN) level. These firewalls are installed in front of individual and/or clusters of Human Machine Interfaces (HMI), Distributed Control Systems (DCS), Programmable Logic Controllers (PLC), or Remote Terminal Units (RTU) control devices that require protection.

Failure to apply the remediations provided below may risk Denial of Service, local code execution, and firmware injection, which could result in service interruption, unexpected device behavior, or device configuration changes to allow malicious network traffic.

Affected Products and Versions

Products	Affected Versions	CVEs
ConneXium Tofino Firewall – part number TCSEFEA23F3F22	Version prior to v03.23	**CVE-2021-30061** **CVE-2021-30064** **CVE-2021-30065** **CVE-2021-30066**
ConneXium Tofino OPC-LSM – part number TCSEFM0000	Version prior to Firewall host version v03.23	**CVE-2021-30062** **CVE-2021-30063**
ConneXium Tofino Firewall – part number TCSEFEA23F3F20/21	All versions	**CVE-2021-30061** **CVE-2021-30064** **CVE-2021-30065** **CVE-2021-30066**

Vulnerability Details

CVE ID: **CVE-2021-30061**

CVSS v3.1 Base Score 6.4 | Medium | CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

An attacker can execute code on the Tofino device by attaching a USB stick with a specially crafted file to the device.

Schneider Electric Security Notification

CVE ID: **CVE-2021-30062**

CVSS v3.1 Base Score 5.3 | Medium | CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N

An attacker can bypass the OPC enforcer using crafted OPC packets.

CVE ID: **CVE-2021-30063**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H

An attacker can cause a denial of service in the OPC enforcer using crafted OPC packets.

CVE ID: **CVE-2021-30064**

CVSS v3.1 Base Score 8.1 | High | CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H

An attacker can access an uncommissioned Tofino device using hardcoded default credentials via SSH.

CVE ID: **CVE-2021-30065**

CVSS v3.1 Base Score 7.5 | High | CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N

An attacker can bypass the Modbus enforcer using crafted Modbus packets.

CVE ID: **CVE-2021-30066**

CVSS v3.1 Base Score 6.8 | Medium | CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An attacker can bypass firmware signature verification on a USB stick and load arbitrary firmware images on the device.

Remediation

Affected Product & Version	Remediation
ConneXium Tofino Firewall – part number TCSEFEA23F3F22	Version v03.23 includes a fix for vulnerabilities **CVE-2021-30061**, **CVE-2021-30064, CVE-2021-30065**, **CVE-2021-30066**. The firmware can be accessed through the Tofino Security user account created at first time registration. Instruction to apply the upgrade can be found in chapter “Upgrading Your Tofino SA” in the device user manual.

Schneider Electric Security Notification

ConneXium Tofino OPC-LSM – part number TCSEFM0000	Version v03.23 of TCSEFEA23F3F22 includes a fix for vulnerabilities **CVE-2021-30062** and **CVE-2021-30063**. Customer using this optional LSM can access to the firmware containing upgraded module through the Tofino Security user account created at first time registration. Note: There is no separate process to upgrade LSM only. Instruction to apply the upgrade can be found in chapter "Upgrading Your Tofino SA" in the device user manual.
ConneXium Tofino Firewall – part number TCSEFEA23F3F20/21	ConneXium Tofino Firewall TCSEFA23F3F20 and TCSEFA23F3F21 products have reached their end of life and are no longer supported. These have been replaced with a newer reference TCSEFA23F3F22. Customers using obsolete Tofino Firewall references are strongly suggested to migrate to the TCSEFA23F3F22. Customers should immediately apply the following mitigations to reduce the risk of exploit: • Restrict physical and logical access to the Tofino devices to trusted personnel. • Connect devices with the Tofino Configurator before leaving them physically unsupervised. • Setup network segmentation and configure the firewall rules to block all unauthorized device.

General Security Recommendations

We strongly recommend the following industry cybersecurity best practices.

- Locate control and safety system networks and remote devices behind firewalls and isolate them from the business network.
- Install physical controls so no unauthorized personnel can access your industrial control and safety systems, components, peripheral equipment, and networks.
- Place all controllers in locked cabinets and never leave them in the "Program" mode.
- Never connect programming software to any network other than the network for the devices that it is intended for.
- Scan all methods of mobile data exchange with the isolated network such as CDs, USB drives, etc. before use in the terminals or any node connected to these networks.

- Never allow mobile devices that have connected to any other network besides the intended network to connect to the safety or control networks without proper sanitation.
- Minimize network exposure for all control system devices and systems and ensure that they are not accessible from the Internet.
- When remote access is required, use secure methods, such as Virtual Private Networks (VPNs). Recognize that VPNs may have vulnerabilities and should be updated to the most current version available. Also, understand that VPNs are only as secure as the connected devices.

For more information refer to the Schneider Electric Recommended Cybersecurity Best Practices document.

For More Information

This document provides an overview of the identified vulnerability or vulnerabilities and actions required to mitigate. For more details and assistance on how to protect your installation, contact your local Schneider Electric representative or Schneider Electric Industrial Cybersecurity Services: https://www.se.com/ww/en/work/solutions/cybersecurity/. These organizations will be fully aware of this situation and can support you through the process.

For further information related to cybersecurity in Schneider Electric's products, visit the company's cybersecurity support portal page:
https://www.se.com/ww/en/work/support/cybersecurity/overview.jsp

About Schneider Electric

At Schneider, we believe **access to energy and digital** is a basic human right. We empower all to **do more with less**, ensuring **Life Is On** everywhere, for everyone, at every moment.

Schneider Electric Security Notification

We provide **energy and automation digital** solutions for **efficiency and sustainability.** We combine world-leading energy technologies, real-time automation, software and services into integrated solutions for Homes, Buildings, Data Centers, Infrastructure and Industries.

We are committed to unleash the infinite possibilities of an **open, global, innovative community** that is passionate with our **Meaningful Purpose, Inclusive and Empowered** values.

www.se.com

Revision Control:

Version 1.0 *11 January 2022*	Original Release

Product Security Office

Digitally signed by Product Security Office
Date: 2022.01.07 14:10:32 -08'00'