Potential Tofino Firmware Signing / Protocol Filtering Evasion / Firewall Bypass

Date: November 6, 2017
Version: 1.0
References: CVE-2017-11400, CVE-2017-11401, CVE-2017-11402

Executive Summary

Three vulnerabilities were reported related to the Tofino, they include:

1. Incomplete signing of Tofino USB upgrade files
2. Protocol filtering evasion with traditional Modbus serial function codes
3. Potential firewall bypass via OPC Enforcer

Details

1. Tofino USB firmware upgrade packages are composed of two files in an archived zip. This includes an update script called appliance_config and a *.tar.sec file. Due to the fact that only the appliance_config file is signed, the .tar.sec file could potentially be modified and used during the update.
2. An attacker can send specially crafted ModBus packets through the Tofino firewall for traditional serial-based function codes. Even with the "sanity check" option enabled, packets with unauthorized function codes or malformed contents may reach protected ICS equipment.
3. An attacker can craft a false OPC dynamic port shift to trigger a firewall rule insert, which in-turn would allow an additional crafted TCP session with fixed source port to circumvent the Tofino firewall.

Impact

1. If an attacker has physical access to the Tofino, the attacker could compromise the appliance with a modified USB upgrade .tar.sec file.
2. For traditional serial-based Modbus Function codes, an attacker can send malformed Modbus frames to an endpoint device.
3. If the Tofino contains an active OPC enforcer, an attacker can trigger a firewall hole that permits a secondary, unrelated TCP session to be established through the firewall.

Affected Products

Brand	Product	Version
Tofino	Tofino Xenon	03.1.00 and lower

Solution

All three vulnerabilities are addressed in version 03.2.00 [1]. Customers are advised to update to this version.

For Help or Feedback

To view all Belden Security Advisories and Bulletins or to report suspected security vulnerabilities, go to https://www.belden.com/security.
For technical support and other requests, please visit https://tofino-support.belden.eu.com.

Acknowledgments

Belden thanks the following for working with us to help protect customers:

- Julien Lenoir of the Airbus CERT Team
- Airbus CERT Team

Related Links

- [1] Firmware download of Tofino Xenon 03.2.00

  Login to https://www.tofinosecurity.com/user/login and navigate to software downloads.

Disclaimer

Revisions

V1.0 (November 6, 2017): Bulletin created.