Multiple Vulnerabilities in Tofino

Date: 2022-01-11

Version: 1.1

References: CVE-2021-30061, CVE-2021-30062, CVE-2021-30063, CVE-2021-30064, CVE-2021-30065, CVE-2021-30066[1]

Executive Summary

Multiple vulnerabilities were discovered in the Tofino, relating to user authentication, USB handling, and two enforcer modules.

Details

CVE	Details	CVSS Score
CVE-2021-30061	An attacker can execute code on the Tofino device by attaching a USB stick with a specially crafted file to the device.	6.4 (CVSS:3.1/AV:P/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2021-30062	An attacker can bypass the OPC enforcer using crafted OPC packets.	5.3 (CVSS:3.1/AV:N/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N)
CVE-2021-30063	An attacker can cause a denial of service in the OPC enforcer using crafted OPC packets.	6.8 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:C/C:N/I:N/A:H)
CVE-2021-30064	An attacker can access an uncommissioned Tofino device using hardcoded default credentials via SSH.	8.1 (CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H)
CVE-2021-30065	An attacker can bypass the Modbus enforcer using crafted Modbus packets.	7.5 (CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N)
CVE-2021-30066	An attacker can bypass firmware signature verification on a USB stick and load arbitrary firmware images on the device.	6.8 (CVSS:3.1/AV:P/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H)

Impact

CVE-2021-30061 and CVE-2021-30066 allow an attacker with physical access to the device to modify its behavior in an arbitrary and persistent manner. CVE-2021-30064 allows an attacker to modify a device that has not yet been connected with a Tofino Configurator, also in an arbitrary and persistent manner. CVE-2021-30062 and CVE-2021-30065 allow an attacker to send crafted OPC Classic and Modbus packets to devices behind the Tofino. CVE-2021-30063 allows an attacker to cause the Tofino to stop switching OPC Classic traffic using crafted packets.

Affected Products

Brand	Product Line / Platform	Product	Version
Hirschmann	Tofino	Xenon TSA	03.2.02 or lower
Hirschmann	Tofino	Argon	All
Hirschmann	EAGLE	EAGLE 20 Tofino	All

Solution

Updates, which address the vulnerability, are available for currently sold products. Customers are advised to update the software.

Brand	Product Line / Platform	Product	Version
Hirschmann	Tofino	Xenon TSA	03.2.03 or higher

Additional countermeasures: Restrict access to the Tofino devices to trusted personnel. Connect devices with the Tofino Configurator before leaving them physically unsupervised.

For Help or Feedback

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

Acknowledgments

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

- Jacob Baines of Dragos

Related Links

- [1] https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30061
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30062
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30063
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30064
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30065
  https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2021-30066

Disclaimer

Revisions

V1.1 (2022-01-11):	Bulletin published.