Tektronix

PRODUCT SECURITY ADVISORY

August 2021

PSIRT Record Number
TEK-PSA-001-0821

OVERVIEW

Ripple20 is a set of vulnerabilities discovered in 2020 in a software library that implemented a TCP/IP stack. The security concerns were discovered by JSOF, which named the collective vulnerabilities for how one company's code became embedded into numerous products.

PSIRT STATEMENT

Tektronix is aware of a set of 19 security vulnerabilities collectively known as “Ripple20” in a third-party TCP/IP stack. Tektronix has identified these vulnerabilities in the Tektronix and Keithley products listed below.

Tektronix-branded products

These vulnerabilities have been identified in certain versions of Intel's Active Management Technology (“AMT”) that are present on Tektronix’s 5 Series, 5 Series Low Profile, 5000 scope, 6 Series, and 6 Series Low Profile products. **Because Tektronix disables the AMT feature on these products, they are not vulnerable as provided by Tektronix.** Tektronix does not have any reason to believe that any of its products have been exploited, but please be aware that if you choose to enable Intel AMT on these products you will risk exposing these vulnerabilities.

Keithley-branded products

Tektronix has identified these vulnerabilities in older versions of firmware on the Keithley-branded products listed below. **These vulnerabilities were patched in firmware revision 1.7.5.** Tektronix recommends upgrading your firmware to at least revision 1.7.5 using the links below.

Product	Firmware Link
2450	MODEL 2450 FIRMWARE REVISION 1.7.5 AND RELEASE NOTES
2460	MODEL 2460 FIRMWARE REVISION 1.7.5 AND RELEASE NOTES
2461	Model 2461 Firmware Revision 1.7.5 and Release Notes
2461-SYS	Model 2461-SYS Firmware Revision 1.7.5 and Release Notes
2470	MODEL 2470 FIRMWARE REVISION 1.7.5 AND RELEASE NOTES
DAQ6510	MODEL DAQ6510 FIRMWARE REVISION 1.7.5 AND RELEASE NOTES
DMM6500	MODEL DMM6500 FIRMWARE REVISION 1.7.5 AND RELEASE NOTES
DMM7510	MODEL DMM7510 FIRMWARE REVISION 1.7.5 AND RELEASE NOTES
DMM7512	Model DMM7512 Firmware Revision 1.7.5 and Release Notes

You should always follow your company’s security practices. In addition, these general practices may also enhance security for Tektronix’s products:

- Only operate Tektronix products in protected or secure networks, limiting remote access.

- When remote access to Tektronix products is required, use only secure remote access methods (for example, your organization’s VPN or other secure method)

   - In accordance with your organization's security policy and/or industry best practices and recognizing that VPNs may also have vulnerabilities and should be updated to the most current version available.

- Whenever possible, segment or isolate Tektronix products from your business network.

- Take additional mitigation steps outlined in CERT vulnerability notice #257161 as appropriate.

ABOUT TEKTRONIX PRODUCT SECURITY

The Product Security Incident Response Team (PSIRT) focuses on identifying, assessing, and analyzing risks associated with security vulnerabilities within Tektronix products. The Tektronix PSIRT is a diverse team of subject matter experts responsible for delivering best in class support to contain and minimize the vulnerability impact.

For more information about Tektronix Product Security and PSIRT, please visit us at https://tek.com/en/support/product-security/advisories

You may also contact us at PSIRT@tektronix.com.

Initial Publication Date	Last Published Date
August, 2021	10/4/2023