Security Advisory 04042022-003

CVE-2022-0778

Initial Publication Date: April 4, 2022

Vulnerability Details:

- CVE-2022-0778
- The BN_mod_sqrt() function, which computes a modular square root, contains a bug that can cause it to loop forever for non-prime moduli. Internally this function is used when parsing certificates that contain elliptic curve public keys in compressed form or explicit elliptic curve parameters with a base point encoded in compressed form.
- OpenSSL advisory https://www.openssl.org/news/secadv/20220315.txt

CVVS Version 3.X Score: 7.5 - High

Summary

This issue affects OpenSSL version 1.1.1m and older. All versions of OpenSSL 1.0.2 that support elliptic curve ciphers are also affected. It was addressed and fixed in OpenSSL 1.1.1n on March 15, 2022.

mPower™ and mLinux operating systems and device-specific firmware versions include OpenSSL and are being updated to OpenSSL 1.1.1n.

- mPower versions prior to mPower 5.3.0 and mPower MTR 5.3.0 are built on OpenSSL 1.0.2X and not supported with upgrades. An upgrade to mPower 5.3.8s-s1 or mPower MTR 5.3.6s-s1 is required.
- mLinux versions prior to mLinux 5.3.0 are built on OpenSSL 1.0.2X and are not supported with upgrades. An upgrade to mLinux 6.0 is required.

Devices and Operating Systems Impacted by CVE-2022-0778

The following table summarizes the devices and operating systems impacted by CVE-2022-0778 and the operating system versions in which this vulnerability will be fixed.

	Device (1) (Model)	Currently Shipping Operating Systems	Updated Operating Systems (including fix)
Bridge	MultiConnect® eCell (MTE)	MTE-LAT6-v208 MTE-LEU6-v208	MTE-LAT6-v211 MTE-LEU6-v211
	MultiConnect® eCell (MTE2)	MTE-Lxxx-v208	MTE-Lxxx-v308
Router	MultiConnect® rCell (MTR)	mPower MTR 5.3.0 mPower MTR 5.3.6	mPower MTR 5.3.6s-s1 mPower MTR 6.0.X
		mLinux 5.3.31	mLinux 6.0.X
Router	MultiConnect® rCell 500 Series (MTR5)	MTR5-LEU2-v417	MTR5-LEU2-v420

	Device [1] (Model)	Currently Shipping Operating Systems	Updated Operating Systems (including fix)
Router	MultiConnect® rCell 600 Series (MTR6)	MTR6-L12G1-v505	MTR6-L12G1-v506
Gateway	Conduit® 300 Series (MTCDT3AC)	mPower 5.4.0	mPower 6.X [2]
Gateway	Conduit® Programmable (MTCDT)	mPower 5.3.5 mPower 5.3.7	mPower 5.3.8s-s1 mPower 6.0.X
		mLinux 5.3.31	mLinux 6.0.X
Base Station	Conduit® IP67 Base Station (MTCDTIP)	mPower 5.3.5 mPower 5.3.7	mPower 5.3.8s-s1 mPower 6.0.X
		mLinux 5.3.31	mLinux 6.0.X
Base Station	Conduit® IP67 200 Series Base Station (MTCDTIP2)	mPower 5.3.5 mPower 5.3.8	mPower 5.3.8s-s1 mPower 6.0.X
Access Point	Conduit® AP Access Point (MTCAP, MTCAP2)	mPower 5.3.5 mPower 5.3.8	mPower 5.3.8s-s1 mPower 6.0.X
		mLinux 5.3.0	mLinux 6.0.X
		mLinux 5.3.4	mLinux 6.0.X
Access Point	MultiConnect® CBRS Wi-Fi AP (MTCAPW)	-	MTCAPW-L12G2-v405

(1) Only MultiTech devices expressly listed in this table are impacted by this advisory

(2) mPower 6.X for use on the Conduit 300 only

Services Impacted by CVE-2022-0778

- MultiTech DeviceHQ® - Cloud-based IoT Device Management
    - MultiTech servers have been updated to address this issue
- MultiTech LENS® - LoRaWAN® Optimized Embedded Network Server and Key Management Toolset
    - MultiTech servers have been updated to address this issue

Schedule

Operating systems can be updated using a full image or differential image

	Downloadable	Device Shipments ***
mLinux 6.0.X	April 2022 *	July 2022
mPower™ 5.3.6s-s1	April 2022 **	April 2022
mPower™ 5.3.8s-s1	April 2022 *	April 2022
mPower™ 6.0.X	April 2022 *	September 2022
mPower™ 6.X	October 2022 *	October 2022
MTE-LAT6-v208	June 2022 **	TBD
MTE-LEU6-v208	June 2022 **	TBD
MTE-Lxxx-v208	June 2022 **	TBD
MTR5-LEU2-v420	June 2022 **	TBD
MTR6-L12G1-v506	June 2022 **	TBD
MTCAPW-L12G2-v405	June 2022 **	TBD

(*) Image updates are downloadable on DeviceHQ and at http://www.multitech.net/developer/downloads/
(**) Image updates are downloadable on device product pages on www.multitech.com
(***) Devices that ship from MultiTech will include the updated operating system

Differential image updates are available through the MultiTech Product Support Portal

- Visit https://support.multitech.com/
- Create a support case and request access to differential file updates
- Not all firmware versions include a differential image update

Customer Action Plan

Devices/Operating Systems: MultiTech recommends the updated operating systems listed above

Additional Information

If you have any questions regarding this Security Advisory, please contact your MultiTech sales representative or visit the technical resources listed below:

World Headquarters – USA

+1 (763) 785-3500 | sales@multitech.com

EMEA Headquarters – UK

+(44) 118 959 7774 | sales@multitech.co.uk

MultiTech Security Advisories

www.multitech.com/landing-pages/security

MultiTech monitors industry news and announcements to identity security issues that may impact our devices and operating systems and strive to provide the information and tools to keep your deployments secure and online.

Subscribe to Future Security Advisories from MultiTech

https://info.multitech.com/acton/form/27728/000e:d-0001/1/-/-/-/-/index.htm

MultiTech Developer Resources

www.multitech.net

An open environment where you can ask development related questions and hear back from MultiTech engineering or a member of this community.

Knowledge Base

http://www.multitech.com/kb.go

Immediate access to support information and resolutions for all MultiTech products.

MultiTech Support Portal

support.multitech.com

Create an account and submit a support case directly to our technical support team.

MultiTech Website

www.multitech.com

Trademarks and Registered Trademarks

MultiConnect, Conduit, mPower, DeviceHQ, LENS, MultiTech and the MultiTech logo are registered trademarks of Multi-Tech Systems, Inc. All other trademarks or registered trademarks are the property of their respective owners.

Revision History

Version	Author	Date	Change Description
-001	DT	04/04/2022	Published version
-002	DT	04/06/2022	Updates made for the following devices: • MultiConnect® eCell (MTE) • MultiConnect® rCell 500 Series (MTR5) • MultiConnect® rCell 600 Series (MTR6) • MultiConnect® CBRS Wi-Fi AP (MTCAPW)
-003	DT	07/14/2022	Updates made throughout