Security Advisory 10122022-001

CVE-2022-2068

Initial Publication Date: October 12, 2022

Vulnerability Details:

CVE-2022-2068

- In addition to the c_rehash shell command injection identified in CVE-2022-1292, further circumstances where the c_rehash script does not properly sanitise shell metacharacters to prevent command injection were found by code review. When the CVE-2022-1292 was fixed it was not discovered that there are other places in the script where the file names of certificates being hashed were possibly passed to a command executed through the shell. This script is distributed by some operating systems in a manner where it is automatically executed. On such operating systems, an attacker could execute arbitrary commands with the privileges of the script. Use of the c_rehash script is considered obsolete and should be replaced by the OpenSSL rehash command line tool. Fixed in OpenSSL 1.1.1p (Affected 1.1.1-1.1.1o).
- OpenSSL advisory: https://www.openssl.org/news/secadv/20220621.txt

CVVS Version 3.X Score: 9.8 Critical

Summary

This issue affects OpenSSL version 1.1.1o. It was addressed and fixed in OpenSSL 1.1.1p on June 21, 2022.

mPower™ operating systems do not use c_rehash script, openssl-rehash script is used

- CVE-2022-2068 does not impact mPower devices

mLinux operating systems use c_rehash script

- CVE-2022-2068 could impact mLinux devices (depending on the customer's application)
- Future mLinux versions will be updated to support OpenSSL version 1.1.1p
  - mLinux 6.1.X will be built using OpenSSL 1.1.1p
  - mLinux 6.0.1 is built using OpenSSL 1.1.1n
  - Previous mLinux versions used OpenSSL 1.1.1b

MultiTech DeviceHQ® - Cloud-based IoT Device Management

- CVE-2022-2068 does not impact MultiTech DeviceHQ
- MultiTech servers have been updated to address this issue

MultiTech LENS® - LoRaWAN® Optimized Embedded Network Server and Key Management Toolset

- CVE-2022-2068 does not impact MultiTech LENS
- MultiTech servers have been updated to address this issue

Customer Action Plan

1. MultiTech recommends that customers update to the operating systems listed in this advisory if c_rehash scripts and CVE-2022-2068 are a concern.

2. Subscribe to MultiTech Security Alerts and Notifications
https://info.multitech.com/acton/form/27728/000e:d-0001/1/-/-/-/-/index.htm

Devices and Operating Systems Impacted by CVE-2022-2068

The following table summarizes the devices and operating systems impacted by CVE-2022-2068 and the operating system versions that will include updates to the OpenSSL version.

	Device (1) (Model)	Currently Shipping Operating Systems	Updated Operating Systems (OpenSSL 1.1.1p)
Gateway	Conduit® Programmable (MTCDT)	mLinux 6.0.1	mLinux 6.1.X
Base Station	Conduit® IP67 Base Station (MTCDTIP)	mLinux 6.0.1	mLinux 6.1.X
Access Point	Conduit® AP Access Point (MTCAP, MTCAP2)	mLinux 6.0.1	mLinux 6.1.X

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

Schedule

	Downloadable	Device Shipments **
mLinux 6.1.X	TBD *	TBD

(*) Image updates are downloadable at http://www.multitech.net/developer/downloads/

(**) Devices that ship from MultiTech will include the updated operating system

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

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	10/12/2022	Published version