Security Advisory 05082023-002

CVE-2023-25201

Initial Publication Date: May 9, 2023

Vulnerability Details:

Advisory ID: USD-2023-0004

- CSRF => RCE in MultiTech Conduit AP MTCAP2-L4E1
- https://herolab.usd.de/en/security-advisories/usd-2023-0004/
- MultiTech Conduit AP MTCAP2-L4E1 is a LoRaWAN access point to provide connectivity of IoT assets. The web interface allows configuration of settings like user management, LoRaWAN, Firewall and custom applications. During an assessment it was discovered that the web interface of the access point is vulnerable to cross-site request forgery attacks (CSRF) attacks. An attacker might be able to cause a user to unknowingly send requests to a vulnerable application. If the user has previously authenticated himself towards the application, those requests will be executed according to the user's privileges. Should the user possess administrative privileges this might enable the attacker to fully compromise the system. A proof-of-concept exploit was written to show remote code execution exploiting the CSRF vulnerability. In order to exploit this vulnerability an attacker needs to fool the user into visiting a specially crafted site of the attacker.
- CVVS Version 3.X Score: 9.6 – Critical

CVE-2023-25201

- Cross Site Request Forgery (CSRF) vulnerability in MultiTech Conduit AP MTCAP2-L4E1-868-042A v.6.0.0 allows a remote attacker to execute arbitrary code via a crafted script upload.

Summary

This issue has been resolved in mPower 6.3.0.

Software & Services – mPower API Services	
mPower API – Updates to cookie parameters API calls allow only first party cookies to be sent using **SameSite=Strict** values to restrict cross-site sharing and prevent cross-site request forgery (CSRF) attacks	Enhancement GP-1896 GP-1763 MTX-4826

To mitigate this issue in legacy versions of mPower, MultiTech has the following recommendations:

1. Never enable the mPower web user interface on the WAN with a static public IP address, especially on the cellular WAN interface.
2. Protect the LAN side of the device from the public Internet by having the MultiTech device on an internal subnet with a firewall or install other edge protection between the LAN and the Internet.
3. Use a browser to connect to the web user interface that is on a computer that is only connected to the internal subnet, preferably on the same subnet/link as the MultiTech device.
4. Avoid using other websites with the same browser that is connected to the MultiTech device.

Devices and Operating Systems Impacted by CVE-2023-25201

The following table summarizes the devices and operating systems impacted by CVE-2023-25201 and the operating system version in which this vulnerability has been fixed.

	Device (1) (Model)	Impacted Operating Systems	Updated Operating Systems (including fix)
Gateway	Conduit® 300 Series (MTCDT3AC)	mPower 5.4.0 mPower 6.2.0	mPower 6.3.0
Gateway	Conduit® Programmable (MTCDT)	mPower 5.3.X mPower 5.2.X mPower 5.1.X	mPower 6.3.0
Gateway	Conduit® IP67 Base Station (MTCDTIP)	mPower 5.3.X mPower 5.2.X mPower 5.1.X	mPower 6.3.0
Gateway	Conduit® AP Access Point (MTCAP, MTCAP2)	mPower 5.3.X mPower 5.2.X mPower 5.1.X	mPower 6.3.0
Gateway	Conduit® AP 300 Series Access Point (MTCAP3)	mPower 6.1.0	mPower 6.3.0
Gateway	Conduit® IP67 200 Series Base Station (MTCDTIP2)	mPower 5.3.X	mPower 6.3.0

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

Schedule

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

	Downloadable *	Device Shipments **
mPower 6.3.0	May 2023	MTCAP3: June 2023 Other Gateway Devices: August 2023
mPower 6.3.0	MTCDT3AC: August 2023	MTCDT3AC: August 2023

(*) Full image updates are downloadable at http://www.multitech.net/developer/downloads/ or on DeviceHQ

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

Customer Action Plan

- Devices/Operating Systems: MultiTech recommends updating to the operating systems listed above.
- Subscribe to MultiTech Security Alerts and Notifications for updates on this and other security-related issues. https://info.multitech.com/acton/form/27728/000e:d-0001/1/-/-/-/-/index.htm

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 identify security issues that may impact our devices and operating systems and strives 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

Conduit, mPower, 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	05/09/2023	Initial version
-002	DT	07/11/2023	Vulnerability details updated mPower 6.3.0 availability updated