Security Advisory 03132023-002

CVE-2023-1017
CVE-2023-1018

Initial Publication Date: March 13, 2023

Vulnerability Details:

Vulnerability Note VU#782720:

- Two buffer overflow vulnerabilities were discovered in the Trusted Platform Module (TPM) 2.0 reference library specification, currently at Level 00, Revision 01.59 November 2019. An attacker who has access to a TPM-command interface can send maliciously-crafted commands to the module and trigger these vulnerabilities. This allows either read-only access to sensitive data or overwriting of normally protected data that is only available to the TPM (e.g., cryptographic keys).

CVE-2023-1017

- An out-of-bounds write vulnerability exists in TPM2.0's Module Library allowing writing of a 2-byte data past the end of TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can lead to denial of service (crashing the TPM chip/process or rendering it unusable) and/or arbitrary code execution in the TPM context.
- CVVS Version 3.X Score: 7.8 – High

CVE-2023-1018

- An out-of-bounds read vulnerability exists in TPM2.0's Module Library allowing a 2-byte read past the end of a TPM2.0 command in the CryptParameterDecryption routine. An attacker who can successfully exploit this vulnerability can read or access sensitive data stored in the TPM.
- CVVS Version 3.X Score: 5.5 - Medium

Summary

After evaluation of all MultiTech products, it is determined MultiTech devices using TPM 2.0 components are not affected by this vulnerability.

Customer Action Plan

- No action required.
- 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 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

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	03/13/2023	Initial release
-002	DT	04/12/2023	Minor updates