UNISPHERE SOLUTIONS

info@unisphere.co.nz
www.unisphere.co.nz

CYBER GUIDANCE ISSUE 0287

NEW FLAWS IN TPM 2.0 LIBRARY

DATE ISSUED: 6th March 2023

IMPACT	LOW	MEDIUM	HIGH
EASE OF EXPLOIT	HARD	MEDIUM	EASY

OVERVIEW

A pair of serious security vulnerabilities have been discovered in the Trusted Platform Module (TPM) 2.0 reference library specification that could potentially lead to information disclosure or privilege escalation.

BREAKDOWN

TPM is a hardware-based technology that provides secure cryptographic functions and physical security mechanisms to resist tampering efforts. It is affected by two buffer overflow vulnerabilities that could allow attackers to access or overwrite sensitive data such as cryptographic keys. The TPM 2.0 is not required for most Windows Security features, however, it is necessary for running Windows 11 because of its boot security measures and supporting Window Hello authentication functions. Researchers from Quarkslab discovered the two vulnerabilities tracked as CVE-2023-1017 and CVE-2023-1018 are a result of lack of necessary length checks, resulting in buffer overflows that could pave the way for local information disclosure or escalation of privileges. An attacker with access to a device built with a vulnerable version of the TPM can trigger these vulnerabilities by sending crafted commands to the TPM allowing access to sensitive data. In some cases, the attacker can also overwrite protected data in the TPM firmware. This may lead to a crash or arbitrary code execution within the TPM.

REMEDIATION STEPS

- Upgrade to the latest version of the software.
- Disable CDP on affected IP Phone devices supporting Link Layer Discovery Protocol (LLDP) to remove the attack vector.

REFERENCES & RESOURCES

Bleeping Computer	https://www.bleepingcomputer.com/news/security/cisco-patches-critical-web-ui-rce-flaw-in-multiple-ip-phones/