Hive Pro

Threat Level

Amber

HiveForce Labs

THREAT ADVISORY

VULNERABILITY REPORT

Two New Vulnerabilities Discovered in TPM 2.0 Library

Date of Publication	Admiralty Code	TA Number
March 06, 2023	A1	TA2023117

Summary

First Seen: February 28, 2023
Affected Product: Trusted Platform Module (TPM) 2.0
Impact: Exploited vulnerable systems may lead to the disclosure of local information or the escalation of privileges.

CVEs

CVE	NAME	PATCH
CVE-2023-1017	Out-of-bounds write vulnerability TPM 2.0	✓
CVE-2023-1018	Out-of-bounds read vulnerability TPM 2.0	✓

Vulnerability Details

#1 The Trusted Platform Module (TPM) 2.0 specification, a hardware-based technology used to provide tamper-resistant secure cryptographic functions, is affected by two buffer overflow vulnerabilities. These vulnerabilities could allow attackers to access or overwrite sensitive data, such as cryptographic keys. The vulnerabilities arise from how the specification processes the parameters for some TPM commands, allowing an authenticated local attacker to exploit them by sending maliciously crafted commands.

#2 The solution for impacted vendors is to move to a fixed version of the specification. Users are recommended to limit physical access to their devices, only use signed applications from reputable vendors, and apply firmware updates as soon as they become available for their devices. While TPM is required for some Windows security features, it is not required for other more commonly used features.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2023-1017	Trusted Platform Module (TPM) before 1.59	cpe:2.3:a:tpm2.0:*:*:*	CWE-787
CVE-2023-1018	Trusted Platform Module (TPM) before 1.59	cpe:2.3:a:tpm2.0:*:*:*	CWE-125

Recommendations

Security Leaders

Asset and vulnerability management solutions should be implemented to ensure that all internet-accessible devices are secure, patched, updated, hardened, and monitored. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize the vulnerability, identify the impacted assets, and patch them through your Command Center. Test your controls with Uni5's Breach & Attack Simulation.

- **All Engineers:** Refer to and action upon the 'Potential MITRE ATT&CK TTPs' & 'Patch Details' on the following pages.

Potential MITRE ATT&CK TTPs

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0004 Privilege Escalation
TA0040 Impact	T1059 Command and Scripting Interpreter	T1190 Exploit Public-Facing Application	T1068 Exploitation for Privilege Escalation
T1485 Data Destruction	T1005 Data from Local System	T1588.006 Vulnerabilities	T1588 Obtain Capabilities

Patch Link

https://trustedcomputinggroup.org/resource/errata-for-tpm-library-specification-2-0/

References

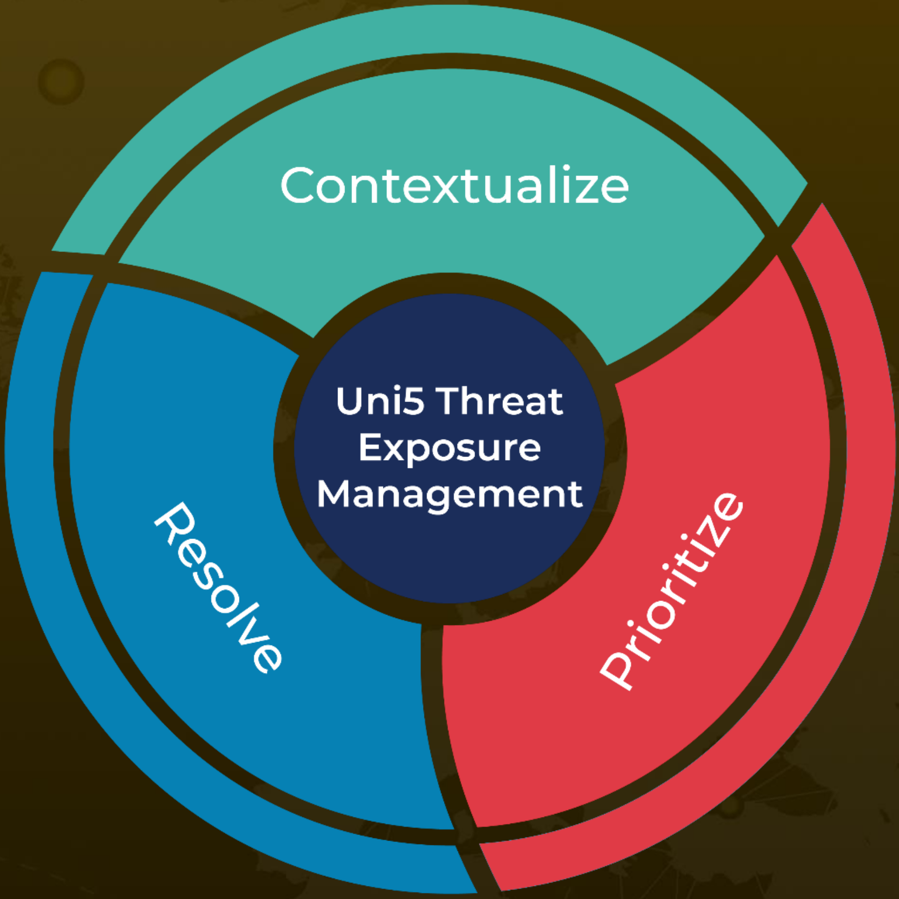
https://www.bleepingcomputer.com/news/security/new-tpm-20-flaws-could-let-hackers-steal-cryptographic-keys/

https://trustedcomputinggroup.org/wp-content/uploads/TCGVRT0007-Advisory-FINAL.pdf

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

March 06, 2023 • 06:30 AM

More at www.hivepro.com