Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

Proof-of-concept released for Windows CryptoAPI vulnerability

Date of Publication	Admiralty Code	TA Number
January 31, 2023	A1	TA2023053

Summary

First appeared: October 11, 2022
Impacted Products: Microsoft Windows and Server
Attack: The critical vulnerability in Windows CryptoAPI allows Spoofing.

CVE

CVE	NAME	PATCH
CVE-2022-34689	Windows CryptoAPI Spoofing Vulnerability	✓

Attack Details

#1 CVE-2022-34689 is a critical vulnerability in Windows CryptoAPI that was publicly announced by Microsoft in October 2022. The vulnerability allows an attacker to masquerade as a legitimate entity by exploiting the assumption that the certificate cache index key, based on MD5, is collision-free.

#2 The attack flow involves two steps: first, the attacker modifies a legitimate certificate and serves it to the victim, and then creates a new certificate with a colliding MD5 and uses it to spoof the original certificate's subject. As a result, the attacker can impersonate a trusted entity and carry out malicious actions such as man-in-the-middle attacks, eavesdropping on sensitive information, and compromising system security.

#3 CryptoAPI is a critical component in Windows for handling cryptography and is widely used by various applications, including browsers, for TLS certificate validation. This makes the vulnerability particularly dangerous, as a successful attack could result in significant security breaches and data loss.

Recommendations

Security Leaders
Phishing simulations and routine education and awareness training and communications rarely account for MFA fatigue and web browser hygiene. Integrate and communicate all lessons learned.

Security Engineers

- **Uni5 Users:** This is an actionable threat advisory in HivePro Uni5. Prioritize and block all indicators attributed to the threat actors and attacks 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' & 'Indicators of Compromise (IoC)' on the following pages.

Potential MITRE ATT&CK TTPs

TA0002 Execution	**TA0005** Defense Evasion	**TA0006** Credential Access	**TA0009** Collection
T1203 Exploitation for Client Execution	**T1204** User Execution	**T1218** System Binary Proxy Execution	**T1027** Obfuscated Files or Information
T1553 Subvert Trust Controls	**T1557** Adversary-in-the-Middle	**T1557.002** ARP Cache Poisoning	

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-34689

References

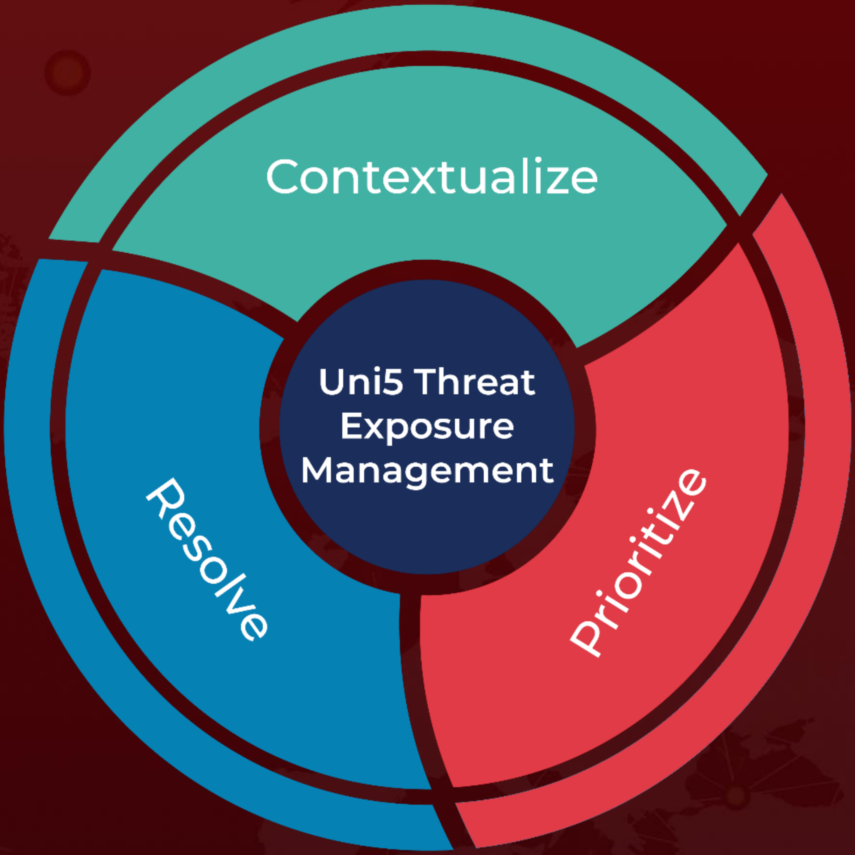
https://www.helpnetsecurity.com/2023/01/26/poc-exploit-cve-2022-34689/

https://www.akamai.com/blog/security-research/exploiting-critical-spoofing-vulnerability-microsoft-cryptoapi

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

January 31, 2023 • 2:30 AM

More at www.hivepro.com