Hive Pro

Threat Level

Red

HiveForce Labs

THREAT ADVISORY

ATTACK REPORT

New Exploit Method Bypasses ProxyNotShell Mitigations

Date of Publication	Admiralty Code	TA Number
December 21, 2022	A1	TA2022309

Summary

First appeared: September 2022
Impacted Products: Microsoft Exchange servers
Attack: Bypassing Microsoft Exchange bug ProxyNotShell mitigations with a new exploit method

CVEs

CVE	NAME	PATCH
CVE-2022-41080	Microsoft Exchange Server Elevation of Privilege Vulnerability	✓
CVE-2022-41082	Microsoft Exchange Server Remote Code Execution Vulnerability	✓
CVE-2022-41040	Microsoft Exchange Server Server-Side Request Forgery Vulnerability	✓
CVE-2022-41123	Microsoft Exchange Server Elevation of Privilege Vulnerability	✓

Attack Details

#1

A new exploit method has been found in the mitigations of the Microsoft Exchange vulnerability ProxyNotShell URL rewrite that allows for remote code execution (RCE) on compromised servers through Outlook Web Access (OWA). The threat actors responsible for this new exploit have been identified as members of the Play ransomware group.

#2

As their common entry vectors, the threat actors used the CVE-2022-41040 and CVE-2022-41082 (ProxyNotShell) vulnerabilities, as well as the CVE-2022-41080 privilege escalation vulnerability on Microsoft Exchange servers. Upon gaining access through these exploits, they leveraged Plink and AnyDesk (remote access tools) to maintain persistence and evade detection on the server.

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

TA0042 Resource Development	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence
TA0005 Defense Evasion	T1059 Command and Scripting Interpreter	T1059.003 Windows Command Shell	T1574.001 Hijack Execution Flow: DLL Search Order Hijacking
T1059.001 Powershell	T1588.006 Vulnerabilities	T1587 Develop Capabilities	T1588 Obtain Capabilities
T1068 Exploitation for Privilege Escalation			

Indicator of Compromise (IOCs)

TYPE	VALUE
URLs	http://179.60.149.28:4427/ http://instance-cmjrni-relay.screenconnect.com

Patch Link

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41082

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41080

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41040

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2022-41123

References

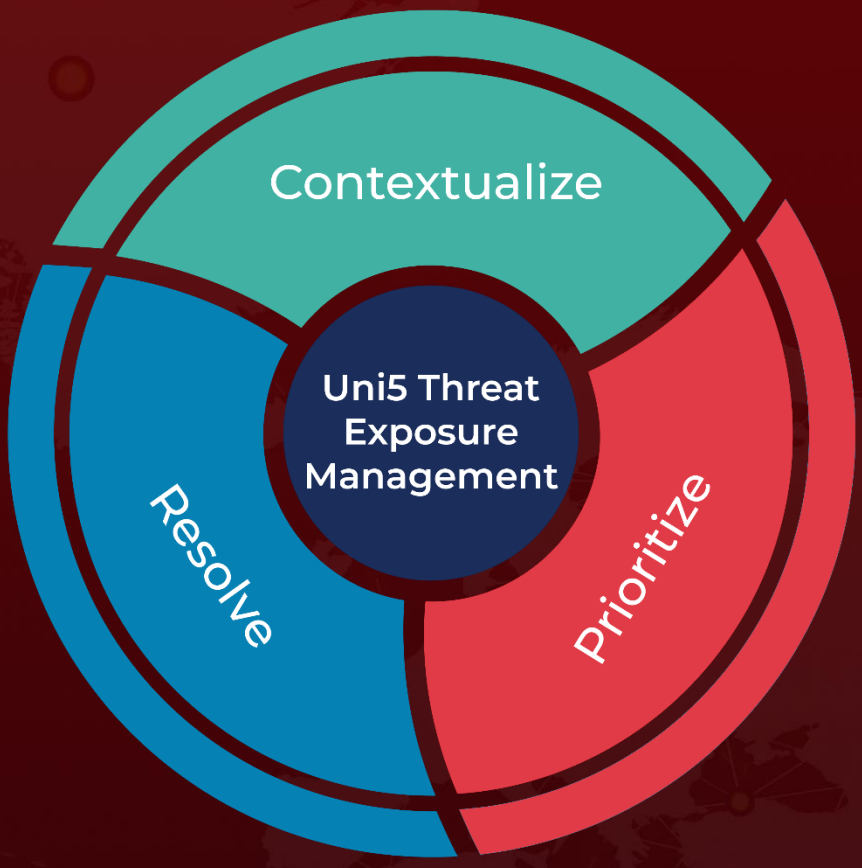
https://twitter.com/Purp1eW0lf/status/1602989967776808961?s=20

https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/

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

December 21, 2022 . 6:30 AM

More at www.hivepro.com