Hive Pro

THREAT ADVISORY

Three zero-days addressed in Microsoft's May 2022 Patch Tuesday

TA2022103

Threat Level RED

Publish Date – May 12, 2022

Microsoft addressed 74 vulnerabilities in their May 2022 Patch Tuesday Security Update. Three of them are zero-days, and one is being exploited in the wild.

The LSA Spoofing vulnerability (CVE-2022-26925) is actively exploited in the wild and allows an unauthenticated attacker to call a method on the LSARPC interface and compel the domain controller to use NTLM to authenticate the attacker. Successful exploitation of the second zero-day vulnerability(CVE-2022-22713) requires an attacker to win a race condition. Third zero-day vulnerability affects the Microsoft Integration Runtime services in the Magnitude Simba Amazon Redshift ODBC Driver.

Organizations are advised the patch all these vulnerabilities as soon as possible to avoid exploitation.

Potential MITRE ATT&CK TTPs are:
TA0042: Resource Development
T1588: Obtain Capabilities
T1588.006: Obtain Capabilities: Vulnerabilities
TA0001: Initial Access
T1190: Exploit Public-Facing Application
TA0006: Credential Access
T1557: Adversary-in-the-Middle

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-26925	Windows: 7 - 11 21H2 and Windows Server: 2008 - 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*	Windows LSA Spoofing Vulnerability	CWE-300
CVE-2022-22713	Windows: 10 - 10 S and Windows Server: 2019 - 2019 2004		Windows Hyper-V Denial of Service Vulnerability	CWE-362
CVE-2022-29972	Microsoft Integration Runtime: 1.0.5144.2 - 5.16.8105.2	cpe:2.3:a:microsoft:microsoft_integration_runtime:*:*:*:*:*:*:*:*	Magnitude Simba Amazon Redshift ODBC Driver injection vulnerability	CWE-94

Patch Link

https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-26925
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-22713
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-29972

References

https://msrc.microsoft.com/update-guide/releaseNote/2022-May