Hive Pro

Threat Level

Amber

THREAT ADVISORY

VULNERABILITY REPORT

Microsoft addresses multiple RCE vulnerabilities in their June 2022 Patch Tuesday

Date of Publication	Admiralty code	TA Number
June 15, 2022	A1	TA2022117

Summary

Microsoft June 2022 Patch Tuesday addressed 55 security flaws. One of them is the Follina which has been addressed in another detailed advisory. Three of them have been rated critical(as per Microsoft) and has been discussed in this advisory.

CVEs

CVE	NAME	PATCH
CVE-2022-30153	Windows LDAP Remote Code Execution Vulnerability	✓
CVE-2022-30161	Windows LDAP Remote Code Execution Vulnerability	✓
CVE-2022-30136	Windows NFS Remote Code Execution Vulnerability	✓

Potential MITRE ATT&CK TTPs

TA0002 Lateral Movement	**TA0002** Execution	**T1204** User Execution	**T1210** Exploitation of Remote Services

Technical Details

#1

The first pair of vulnerabilities, CVE-2022-30153 and CVE-2022-30161, can be used by attacker to trick a victim connected to the network to connect to a malicious LDAP server using their LDAP client application. The Third vulnerability, CVE-2022-30136 could be used by an attacker to execute code remotely by making an unauthenticated, specially crafted call to a Network File System (NFS) service.

#2

All these vulnerabilities have been fixed by Microsoft in there June 2022 patch Tuesday and organizations should upgrade there system as soon as possible to avoid exploitation.

Vulnerability Details

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2022-30153	Windows: 7 - XP Windows Server: 20H2 - 2022	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*:*	CWE-20
CVE-2022-30161	Windows: 7 - XP Windows Server: 20H2 - 2022	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*:*	CWE-20
CVE-2022-30136	Windows Server: 2012 - 2019 2004	cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	CWE-20

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30153
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30161
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-30136

References

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

What Next?

Book a free demo with **HivePro Uni5** to check your exposure to this advisory. HivePro Uni5 is a Threat Exposure Management Solution that proactively reduces an organization's attack surface before it gets exploited.

At Hive Pro we take a long hard look at your vulnerabilities so you can bolster your defenses and fine-tune your offensive cybersecurity tactics.

REPORT GENERATED ON

June 15, 2022 • 4:45 AM

More at www.hivepro.com