Hive Pro

THREAT ADVISORY

Microsoft Patch Tuesday April 2022 addressed two zero-day vulnerabilities

TA2022091

Threat Level RED

Publish Date – April 13, 2022

Microsoft addressed 128 vulnerabilities in there April patch Tuesday update. Two of them have been categorized as zero-day vulnerabilities. One of the two zero-days is exploited-in-the-wild as well.

The vulnerability, CVE-2022-24521, has been exploited in the wild. By exploiting this flaw in the Windows Common Log File System (CLFS) driver, an attacker can escalate privileges. The second zero-day is CVE-2022-26904, which is discovered in the Windows User Profile Service also permits the escalation of privileges. Despite being listed as more likely to be exploited, it has a high attack complexity, and successful exploitation requires an attacker to win a race condition.

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
TA0004: Privilege Escalation
T1068: Exploitation for Privilege Escalation

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2022-26904	Windows: 7 - 11 21H2 and Windows Server: 2008 – 2022	cpe:2.3:o:microsoft:windows:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:*:*:*:*:*:*:*:*:*	Windows User Profile Service Elevation of Privilege Vulnerability	CWE-362
CVE-2022-24521			Windows Common Log File System Driver Elevation of Privilege Vulnerability	CWE-119

Patch Links

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-24521
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-26904

References

https://www.cisa.gov/uscert/ncas/current-activity/2022/04/12/microsoft-releases-april-2022-security-updates