Hive Pro

THREAT ADVISORY

Microsoft's privilege escalation vulnerability that refuses to go away

TA2022076

Threat Level AMBER

Publish Date – March 25, 2022

After seven months, a vulnerability that was addressed in August 2021 patch Tuesday remained unpatched. This locally exploited vulnerability is tracked as CVE-2021-34484 and affects the Windows User Profile Service. While Proof-of-concept is been available for some time now, it is not been actively exploited in the wild.

This Elevation of Privilege vulnerability was found by renowned researcher Abdelhamid Naceri and reported to Microsoft, which addressed it in their August 2021 release. Naceri noted that Microsoft's fix was incomplete soon after it was issued and presented a proof of concept (POC) that bypassed it on all Windows versions. That is when the 0patch team, published an unofficial security update for all Windows versions and made it available for free download to all registered users. Microsoft then patched this security flaw in their January 2022 release, tracking it as CVE-2022-21919. Naceri, on the other hand, discovered a way around this second patch. However, Microsoft's second attempt to fix the bug altered the "profext.dll" file, resulting in the removal of the unofficial workaround of 0patch from everyone who had installed the January 2022 Windows updates.

Organizations could apply the 0patch unofficial patch to patch this vulnerability using the steps given below:
1. Update Windows 10 to the latest March 2022 patch.
2. Create a free account in 0patch Central
3. Install and register the 0patch Agent
4. An automated micro-patching process will initiate to apply this patch.

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
TA0005: Defense Evasion
T1548: Abuse Elevation Control Mechanism

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-34484	Microsoft Windows versions 7 SP1, 8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, RT 8.1, Server 20H2, Server 2004, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016, Server 2019	cpe:2.3:o:microsoft:*:*:*:*:*:*:*:*:*	Windows User Profile Service Elevation of Privilege Vulnerability	CWE-269
CVE-2022-21919	Microsoft Windows versions 7 SP1, 8.1, 10, 10 20H2, 10 21H1, 10 21H2, 10 1607, 10 1809, 10 1909, 11, RT 8.1, Server 20H2, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016, Server 2019, Server 2022	cpe:2.3:o:microsoft:*:*:*:*:*:*:*:*:*	Windows User Profile Service Elevation of Privilege Vulnerability	CWE-269

References

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-21919
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34484
https://www.bleepingcomputer.com/news/microsoft/windows-zero-day-flaw-giving-admin-rights-gets-unofficial-patch-again/
https://blog.0patch.com/2022/03/a-bug-that-doesnt-want-to-die-cve-2021.html