Hive Pro

THREAT ADVISORY

Microsoft patches a vulnerability that was used in MysterySnail RAT Campaign

TA202142

Threat Level RED

Publish Date – Oct 13, 2021

An APT espionage campaign leveraged a zero-day exploit for Microsoft Windows to escalate privileges and obtain access to Windows servers. The exploit chain culminated in the installation of a newly discovered remote access trojan (RAT) called MysterySnail on compromised servers with the purpose of stealing data. The flaw (CVE-2021-40449) was fixed as part of Microsoft's October Patch Tuesday upgrades, which were released this week.

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name
CVE-2021-40449	Microsoft Windows 7 SP1, 8.1, 10, 10 20H2, 10 21H1, 10 1607, 10 1809, 10 1909, 10 2004, 11, RT 8.1, Server 20H2, Server 2004, Server 2008 R2 SP1, Server 2008 SP2, Server 2012, Server 2012 R2, Server 2016, Server 2019, Server 2022	cpe:2.3:o:microsoft:windows_7:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_8.1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:21h1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1607:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1809:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:1909:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_10:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows:11:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:sp2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2012:r2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:*:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server:2022:*:*:*:*:*:*:*	Microsoft Windows Win32k privilege escalation

Actor Details

Name	Known as	Origin	Target Location	Target Sector
IronHusky	BBCY-TA1	China	Mongolia, Russia.	Defense, Financial, Government, IT

Indicators of Compromise(IoCs)

Type	Value
MD5 Hash	e2f2d2832da0facbd716d6ad298073ca
SHA1 Hash	ecdec44d3ce31532d9831b139ea04bf48cde9090
SHA2 Hash	b7fb3623e31fb36fc3d3a4d99829e42910cad4da4fa7429a2d99a838e004366e
Domains	www[.]disktest[.]com www[.]runblerx[.]com http[.]ddspadus[.]com

Patch Link

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40449

References

https://securelist.com/mysterysnail-attacks-with-windows-zero-day/104509/