Hive Pro

THREAT ADVISORY

Russian threat actors leveraging misconfigured multifactor authentication to exploit PrintNightmare vulnerability	TA2022066
Threat Level RED	**Publish Date –** Mar 18, 2022

The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have issued an alert for enterprises that Russian state-sponsored cyber attackers have obtained network access by exploiting default MFA protocols and a known vulnerability.

Russian state-sponsored cyber attackers got initial access to the target organization by using compromising credentials and registering a new device in the organization's Duo multi-factor authentication (MFA). The actors obtained the credentials using a brute-force password guessing attack, which provided them with access to a victim account with a basic, predictable password. The victim account had been unenrolled from Duo after a long period of inactivity, but it had not been deactivated in Active Directory. The actors were able to enroll a new device for this account, satisfy the authentication requirements, and get access to the victim network since Duo's default configuration settings allow for the re-enrollment of a new device for inactive accounts. Using the stolen account, Russian state-sponsored cyber attackers gained administrator rights by exploiting the "PrintNightmare" vulnerability (CVE-2021-34527). Furthermore, the cyber actors were able to obtain required material by moving laterally to the victim's cloud storage and email accounts.

The organizations can apply the following mitigations:

- To prevent against "fail open" and re-enrollment scenarios, enforce MFA and examine configuration restrictions.
- Assure that inactive accounts are deactivated consistently across the Active Directory and MFA systems.
- Ensure that inactive accounts are deactivated equally across Active Directory, MFA systems, and other systems.
- Update software such as operating systems, apps, and hardware on a regular basis.

The Mitre TTPs used in the current attack are:
TA0001 - Initial Access
TA0003 - Persistence
TA0004 - Privilege Escalation
TA0005 - Defense Evasion
TA0006 - Credential Access
TA0007 - Discovery
TA0008 - Lateral Movement
TA0009 - Collection
T1078: Valid Accounts
T1133: External Remote Services
T1556: Modify Authentication Process
T1068: Exploitation for Privilege Escalation
T1112: Modify Registry
T1110.001: Brute Force: Password Guessing
T1003.003: OS Credential Dumping: NTDS
T1018: Remote System Discovery
T1560.001: Archive Collected Data: Archive via Utility

Hive Pro

THREAT ADVISORY

Vulnerability Details

CVE ID	Affected Products	Affected CPE	Vulnerability Name	CWE ID
CVE-2021-34527	Microsoft Windows 10. 7. 8.1, Windows Server 2008, 2012, 2016, 2019	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_7:-:sp1:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_8.1:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_rt_8.1:-:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:-:sp2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2008:r2:sp1:*:*:*:*:x64:*:*, 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_2016:20h2:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2016:2004:*:*:*:*:*:*:*, cpe:2.3:o:microsoft:windows_server_2019:-:*:*:*:*:*:*:*	Windows Print Spooler Remote Code Execution	CWE-269

Indicators of Compromise (IoCs)

Type	Value
URLs	hxxps://cdn.discordapp[.]com/attachments/932413459872747544/938291977735266344/putty.exe hxxps://cdn.discordapp[.]com/attachments/932413459872747544/938317934026170408/puttyjejfrwu.exe, hxxp://185.244.41[.]109:8080/upld/, hxxp://eumr[.]site/load74h74830.exe, eumr[.]site, mariaparsons10811@gmail[.]com,
IPs	45.32.137[.]94 191.96.121[.]162 173.239.198[.]46 157.230.81[.]39
SHA-1	3eec65c8ac25682d9e7d293ca9033c8a841f4958, d77421caae67f4955529f91f229b31317dff0a95, ef5400f6dbf32bae79edb16c8f73a59999e605c7, 3847ca79b3fd52b105c5e43b7fc080aac7c5d909

Patch

https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527

References

https://www.cisa.gov/uscert/ncas/alerts/aa22-074a