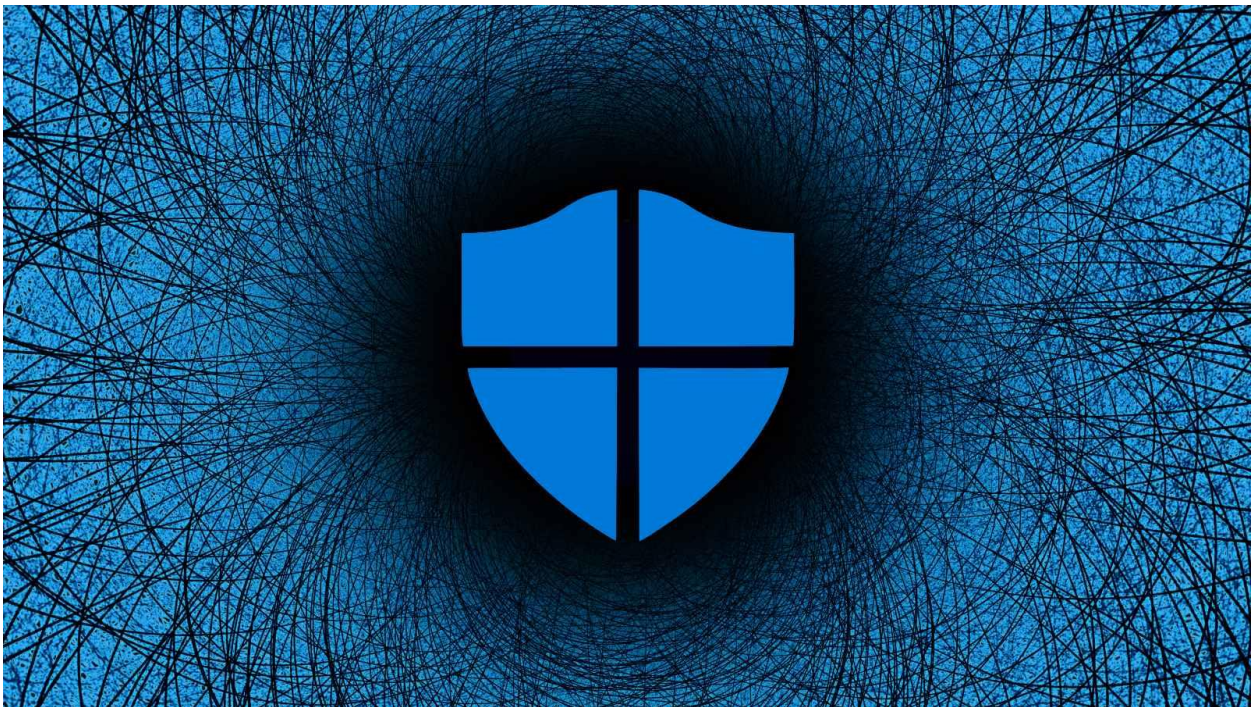
Microsoft Defender for Identity now detects PrintNightmare attacks



Microsoft has added support for PrintNightmare exploitation detection to Microsoft Defender for Identity to help Security Operations teams detect attackers' attempts to abuse this critical vulnerability.

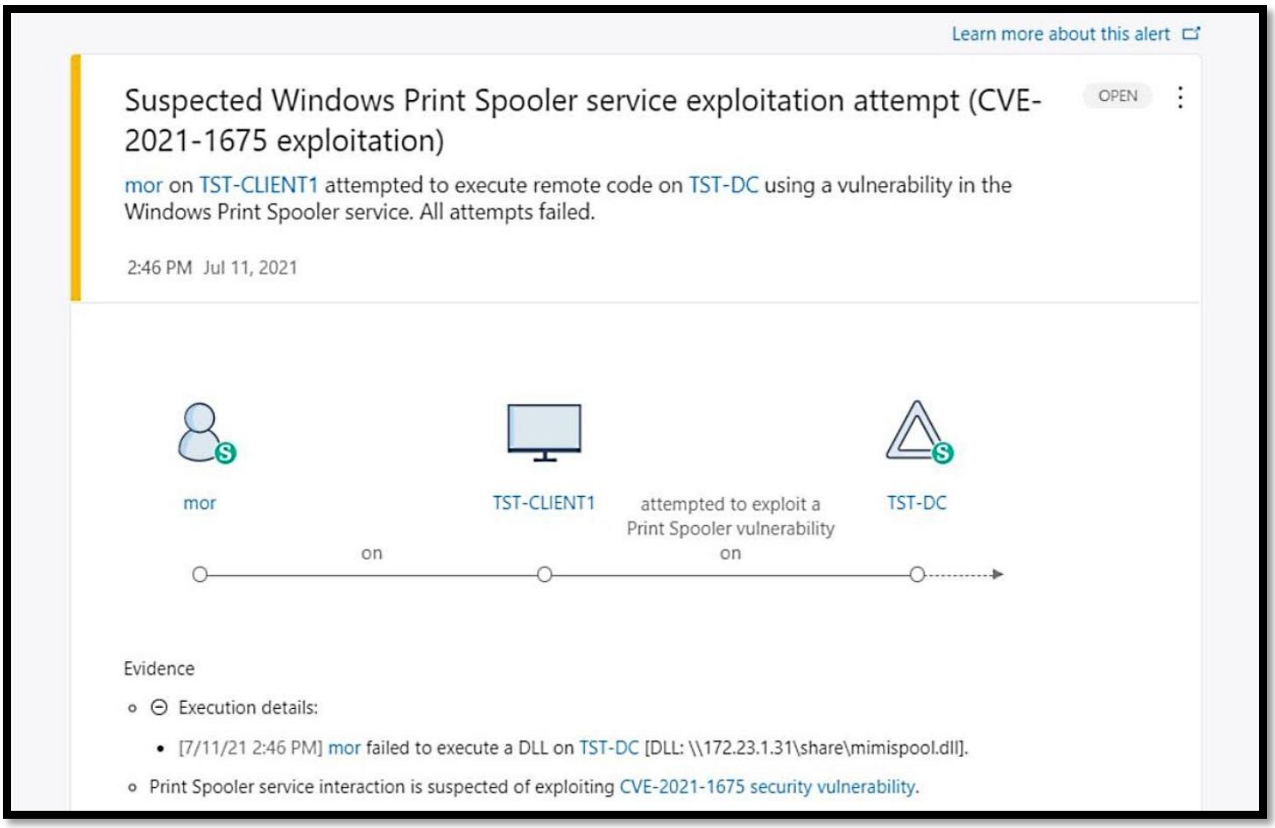
As revealed by Microsoft program manager Daniel Naim, Defender for Identity now identifies Windows Print Spooler service exploitation (including the actively exploited CVE-2021-34527 PrintNightmare bug) and helps block lateral movement attempts within an org's network.

If successfully exploited, this critical flaw enables attackers to take over affected servers by elevating privileges to Domain Administrator, stealing domain credentials, and distribute malware as a Domain Admin via remote code execution (RCE) with SYSTEM privileges.

Microsoft Defender for Identity (previously known as Azure Advanced Threat Protection or Azure ATP) is a cloud-based security solution that leverages on-premises Active Directory signals.

This allows SecOps teams to detect and investigate compromised identities, advanced threats, and malicious insider activity targeting enrolled orgs.

Defender for Identity is bundled with Microsoft 365 E5 but, if you don't have a subscription already, you can get a Security E5 trial right now to give this new feature a spin.



Microsoft Defender for Identity detecting PrintNightmare exploitation attempt (Daniel Naim)

Last week, Microsoft clarified the PrintNightmare patch guidance and shared the steps needed to correctly patch the critical vulnerability after several security researchers tagged the patches issued to address the bug were incomplete.

CISA also issued an emergency directive on Tuesday, ordering federal agencies to mitigate the actively exploited PrintNightmare vulnerability on their networks.

In related news, Defender for Identity was updated in November to detect Zerologon exploitation as part of on-premises attacks attempting to this critical vulnerability.

Microsoft will roll out a another update later this month which will enable security operations (SecOps) teams to block attack attempts by locking compromised users' Active Directory accounts.

New Windows Print Spooler vulnerability

On Thursday evening, Microsoft shared mitigation guidance on a new Windows Print Spooler elevation of privilege vulnerability tracked as CVE-2021-34481 and discovered by Dragos security researcher Jacob Baines.

Unlike PrintNightmare, this security bug can only be exploited by attackers with local access to vulnerable systems to gain elevated privileges.

"The attack is not really related to PrintNightmare. As you know, PN can be executed remotely and this is a local only vulnerability," Baines told BleepingComputer.

While Microsoft shared very little info regarding this bug (including what versions of Windows are vulnerable), Baines said that the security flaw is printer driver-related.

Redmond is still investigating this vulnerability and working on security updates to address the underlying Windows Print Spooler service weaknesses.

Until a CVE-2021-34481 patch is available, Microsoft advises admins to disable the Print Spooler service on Windows devices exposed to attacks.

References:

https://www.bleepingcomputer.com/news/security/microsoft-defender-for-identity-now-detects-printnightmare-attacks/

https://news-block.com/microsoft-defender-for-identity-now-detects-printnightmare-attacks/

https://technewsterminal.com/microsoft-defender-for-identity-now-detects-printnightmare-attacks/

https://stimuluscheckup.com/2021/07/16/microsoft-defender-for-identity-now-detects-printnightmare-attacks/