Defender for Identity detects PrintNightmare vulnerability, reducing risk for Print Spooler

Microsoft helped Defender for Identity detect the PrintNightmare exploit to help the Security Operations team detect hacker attacks.

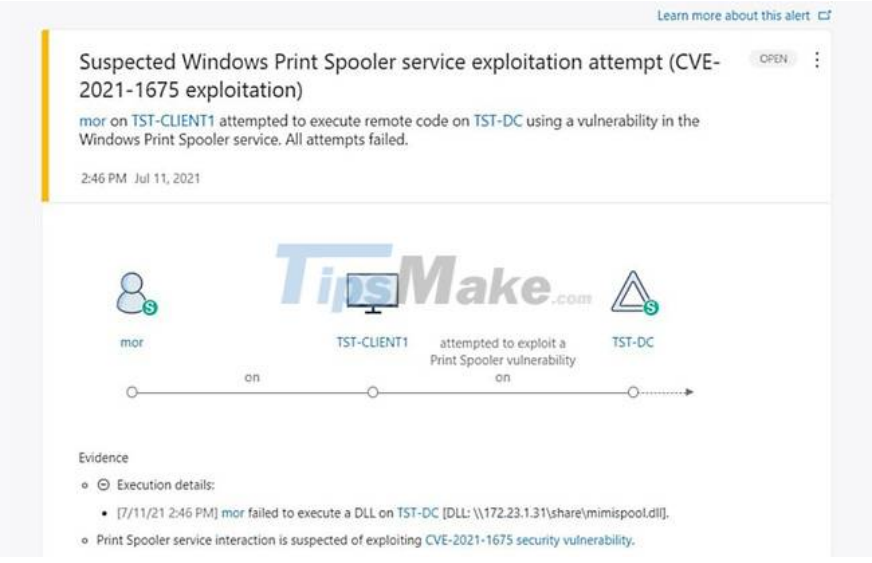
According to Daniel Naim, Microsoft program manager, Defender for Identity can now detect exploits of the Print Spooler service using the PrintNightmare vulnerability (CVE-2,021-34.527) and help prevent attacks inside the networks of Microsoft servers. organization.

If successfully exploited, this critical vulnerability grants Domain Administrator elevated privileges, steals domain credentials, and distributes malware as a Domain Administrator via RCE, with SYSTEM privileges. This allows an attacker to take over the affected servers.

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

This enables SecOps security operations teams to detect and investigate compromised identities, advanced threats, and malicious insider activity targeting registered organizations.

You need to subscribe to the Microsoft 365 E5 plan to use Defender for Identity. But if you haven't signed up yet, you can get a trial of Security E5 now to power this new feature.



Last week, Microsoft clarified the PrintNightmare patch guide and shared the steps needed to patch the critical vulnerability correctly after some security researchers discovered the patch could still be "barred". .

CISA also requires federal agencies to mitigate the actively exploited PrintNightmare vulnerability on their networks.

Defender for Identity was updated in November to detect the Zerologon exploit as part of on-premises attacks targeting this critical vulnerability.

Microsoft will roll out another update later this month that will allow SecOps to thwart attack attempts by locking down compromised users' Active Directory accounts.

You finished reading the article "**Defender for Identity detects PrintNightmare vulnerability, reducing risk for Print Spooler**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

© 2019 TipsMake.com