Matrixforce®

www.matrixforce.com

Incident Response

Incident Date(s): 7/28/2021

Description: Microsoft reported a potential PetitPotam or NTLM Relay attack vulnerability that could be used to steal administrator and user account credentials on July 28, 2021.

At this time, Microsoft notes this attack has not been exploited in the wild and has no assessment about the exploit severity. Attackers must gain access to the local network to exploit this vulnerability and mitigation steps must be tested as disabling NTLM block logon to legacy applications and server operating systems.

Network security Restrict NTLM in this domain (Windows 10) - Windows security | Microsoft Docs

Response: Support immediately:

- Verified and confirmed no malicious activity in security logs on supported customer networks.
- Published this incident response on our website, blog, and social media:
  Incident Response (matrixforce.com)
  Incident Response Readiness – Matrixforce Pulse
  Incident Response Beforehand | LinkedIn

We will be implementing this mitigation internally today. Legacy Windows Server 2008 must be removed or added to mitigation exclusions for clients to accept potential risk. **Software vendors should also be publishing whether their application is at risk and must be excluded.** Support will coordinate with clients over the next month to mitigate each unique environment.