Protect your Windows systems from critical NTLM Relay vulnerability

Review Microsoft suggested actions and configure as appropriate immediately to mitigate ADV210003.

Your action is required

August 6, 2021 -- As a valued supplier, Intel wants you to be aware of a Microsoft Security Advisory ADV210003, also known as PetitPotam. This critical vulnerability is a NTLM Relay Attack that impacts Windows domain controllers or other Windows servers for all machines running Windows Server 2008, Windows Server 2008 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022.

What "PetitPotam" does

If exploited, this vulnerability could allow:

- IP loss and the ability of bad actors to impersonate Intel or a supplier
- Stolen user credentials transferred between a client and server allowing attackers to gain inappropriate access to resources.

Learn more in this release from Microsoft – KB5005413

What you need to do

- Intel requests that you review the Microsoft mitigation options in KB5005413 and take appropriate steps immediately.

Failure to appropriately address this vulnerability could result in serious system compromise and spoofing attacks.

Need help?

For more information, please visit Microsoft's Credential Relaying Attacks on Integrated Windows Authentication page

---