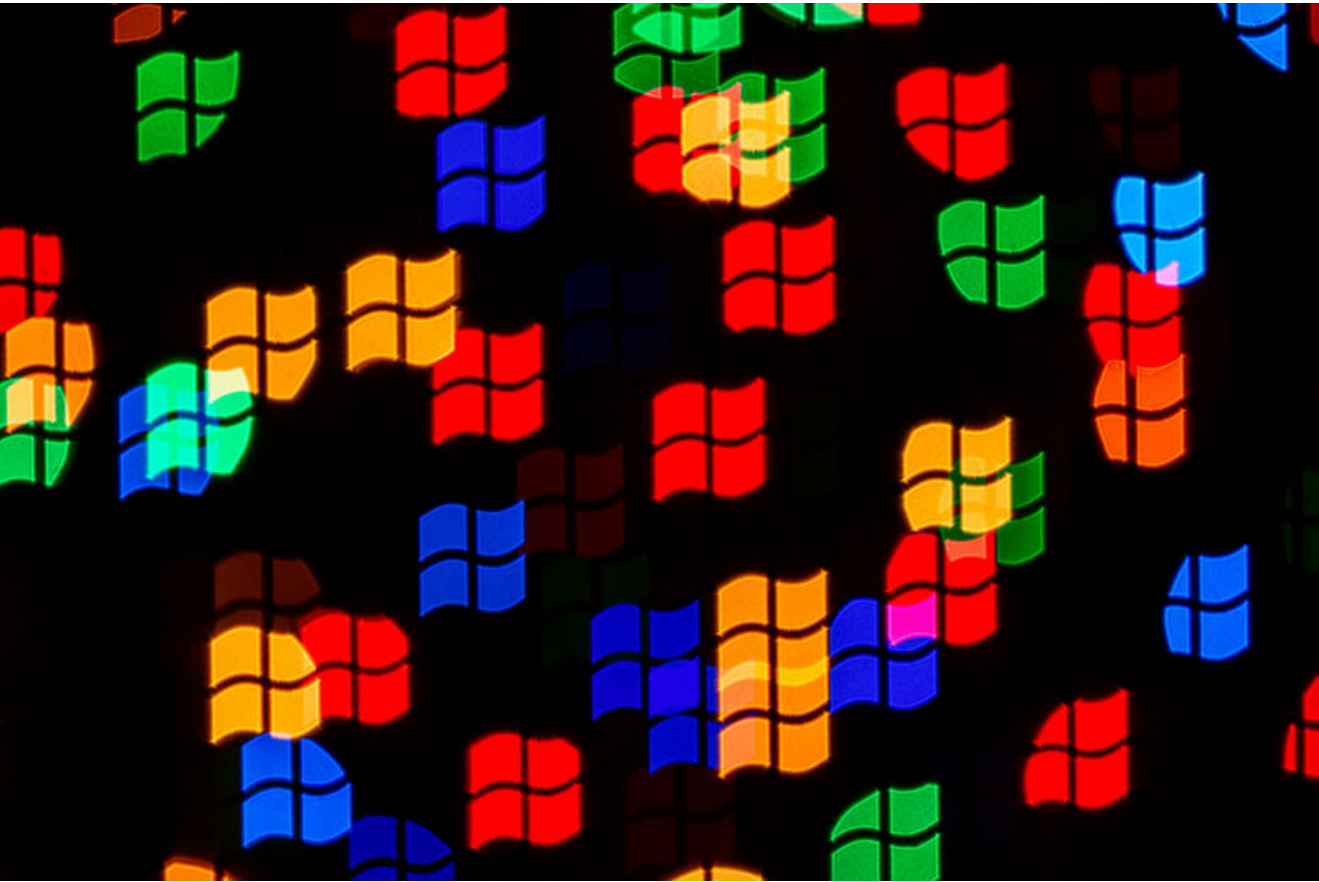



# Microsoft Rushes Fix for ‘PetitPotam’ Attack PoC





Author:

Tom Spring

July 26, 2021 / 3:33 pm

2 minute read

Share this article:

f

✕

...

Microsoft releases mitigations for a Windows NT LAN Manager exploit that forces remote Windows systems to reveal password hashes that can be easily cracked.

Microsoft was quick to respond with a fix to an attack dubbed “PetitPotam” that could force remote Windows systems to reveal password hashes that could then be easily cracked. To thwart an attack, Microsoft recommends system administrators stop using the now deprecated Windows NT LAN Manager (NTLM).

Security researcher Gilles Lionel first identified the bug on Thursday and also published proof-of-concept (PoC) exploit code to demonstrate the attack. The following day, Microsoft issued an advisory that included workaround mitigations to protect systems.

The PetitPotam bug is tied to the Windows operating system and the abuse of a remote access protocol called Encrypting File System Remote Protocol (MS-EFSRPC). The protocol is designed to allow Windows systems to access remote encrypted data stores, allowing for management of the data while enforcing access control policies.

Threatpost Today! Daily headlines delivered to your inbox


Subscribe now

The PetitPotam PoC is a form of manipulator-in-the-middle (MitM)




- INFOSEC INSIDER
- Securing Your Move to the Hybrid Cloud


August 1, 2022


- Why Physical Security Maintenance Should Never Be an Afterthought


July 25, 2022


- Conti’s Reign of Chaos: Costa Rica in the Crosshairs


July 20, 2022


- How War Impacts Cyber Insurance

July 12, 2022


- Rethinking Vulnerability Management in a Heightened Threat Landscape

July 11, 2022



 Cybersecurity for your growing business

According to Lionel, this forces the targeted computer to initiate an authentication procedure and share its authentication details via NTLM.

## NTLM: Persona Non Grata Protocol

Because the NTLM protocol is an insufficient authentication protocol that’s nonetheless used to relay authentication details, hashed passwords can be scooped up by an attacker and later cracked offline with minimal effort. NTLM has a long list of criticisms that [date back to 2010](#), when even then it was seen as an insufficient authentication protocol.

“NTLM is susceptible to relay attacks, which allows actors to capture an authentication and relay it to another server, granting them the ability to perform operations on the remote server using the authenticated user’s privileges,” wrote researchers at Preempt in [a 2019 report](#).

## Attack Scenario

According to Lionel, this similar scenario can be played out with a PetitPotam attack. He demonstrated how a PetitPotam attack can be chained to an exploit targeting Windows Active Directory Certificate Services (AD CS), which provides public key infrastructure (PKI) functionality.

Researchers at Truesec break it down further in a [blog post published Sunday](#).

“An attacker can target a Domain Controller to send its credentials by using the MS-EFSRPC protocol and then relaying the DC [domain controller] NTLM credentials to the Active Directory Certificate Services AD CS Web Enrollment pages to enroll a DC certificate. ... This will effectively give the attacker an authentication certificate that can be used to access domain services as a DC and compromise the entire domain.”

## PetitPotam Mitigation Options

In response to the public availability of the PoC, Microsoft was quick to respond, outlining several mitigation options. For starters, Microsoft recommends disabling NTLM authentication on Windows domain controllers. It also suggests enabling the Extended Protection for Authentication (EPA) feature on AD CS services.

“To prevent NTLM Relay Attacks on networks with NTLM enabled, domain administrators must ensure that services that permit NTLM authentication make use of protections such as [Extended Protection for Authentication \(EPA\)](#) or signing features such as SMB signing,” wrote Microsoft. “PetitPotam takes advantage of servers where Active Directory Certificate Services (AD CS) is not configured with protections for NTLM Relay Attacks. The mitigations outlined in [KB5005413](#) instruct customers on how to protect their AD CS servers from such attacks.”

Microsoft also added that companies are vulnerable to a PetitPotam attack if NTLM authentication is enabled in their domains and/or they’re using AD CS with the services “Certificate Authority Web Enrollment” and “Certificate Enrollment Web Service.”

and the Threatpost community.

Share this article:

Vulnerabilities

SUGGESTED ARTICLES



Ransomware Attacks are on the Rise

Lockbit is by far this summer’s most prolific ransomware group, trailed by two offshoots of the Conti group.

August 26, 2022



Cybercriminals Are Selling Access to Chinese Surveillance Cameras

Tens of thousands of cameras have failed to patch a critical, 11-month-old CVE, leaving thousands of organizations exposed.

August 25, 2022



Firewall Bug Attack Triggers CISA Warning

CISA is warning PAN-OS is under attack and needs to be patched.

August 23, 2022



The First Stop For Security News

[Home](#) / [About Us](#) / [Contact Us](#) / [RSS Feeds](#)

Copyright © 2024 Threatpost • [Privacy Policy](#) • [Terms and Conditions](#)

TOPICS

- [Black Hat](#) [Breaking News](#) [Cloud Security](#) [Critical Infrastructure](#) [Cryptography](#) [Facebook](#) [Government](#) [Hacks](#) [IoT](#) [Malware](#) [Mobile Security](#) [Podcasts](#) [Privacy](#) [RSAC](#) [Security Analyst Summit](#) [Videos](#) [Vulnerabilities](#) [Web Security](#)

We use cookies to make your experience of our websites better. By using and further navigating this website you accept this. Detailed information about the use of cookies on this website is available by clicking on more information.

ACCEPT AND CLOSE