

Forum:[Hack Forums](#)

Thread: [CVE-2026-24294 | Modern \(shittier\) eternal blue](#)

Biggy_Asian - May 26, 2026, 4:49 pm

POC : <https://github.com/0xNDI/CVE-2026-24294>

This is a modern day windows 11 SMB (Server Message Block) exploit which allows remote execution on servers, however do not forget it also has SYSTEM "Local privilege escalation" along side its RCE capabilities. It is a month old and I am a little late however does not mean you can go use shodan and scrape the internet for pwnable devices.

Readme cypypasta:

Code Attack flow:

LSASS (SYSTEM) --NTLM--? SMB Client --TCP:12345--? smbserver.py (ours)

|
? relay NTLM blob

SMB Service (:445) ?----- ntlmrelayx.py

<- SYSTEM session

Code Requirements:

Windows Server 2025 target (basically windows 11 like how 2022 is basically 10)

Python 3 with Impacket

PetitPotam.exe (build from source with Visual Studio, see PetitPotam/)

go look at the [readme](#).

MadScientist - May 26, 2026, 5:15 pm

(May 26, 2026 04:49 PM)Biggy_Asian Wrote: [\[CITE\]](#) POC :

<https://github.com/0xNDI/CVE-2026-24294>

This is a modern day windows 11 SMB (Server Message Block) exploit which allows remote execution on servers, however do not forget it also has SYSTEM "Local privilege escalation" along side its RCE capabilities. It is a month old and I am a little late however does not mean you can go use shodan and scrape the internet for pwnable devices.

Readme cypypasta:

Code Attack flow:

LSASS (SYSTEM) --NTLM--? SMB Client --TCP:12345--? smbserver.py (ours)

|
? relay NTLM blob

SMB Service (:445) ?----- ntlmrelayx.py

<- SYSTEM session

Code Requirements:

Windows Server 2025 target (basically windows 11 like how 2022 is basically 10)
Python 3 with Impacket
PetitPotam.exe (build from source with Visual Studio, see PetitPotam/)
go look at the [readme](#).
You test it out?

?Border?ineExtr(A) - May 26, 2026, 5:24 pm

Port 12345 a hard, definitive OPEN ACCESS or could be different, like 13579 (odds) & 02468 (evens). From what I know, port limit 50k is a bearing threshold, greater success with lower tiers for easy routing 10'000-20'000.

Totally misread as 'potatoes' LMAO.

Biggy_Asian - May 27, 2026, 3:19 pm

(May 26, 2026 05:15 PM)MadScientist Wrote: [\[CITE\]](#) You test it out?
No, I found it cool and thought to share it just because.

DramaKing - May 29, 2026, 9:10 am

This is LPE, not RCE. It requires local access to the target.