From Man-in-the-Middle to Privesc and RCE: Exploiting the Netlogon Protocol

Tom Tervoort
Outline

1. Introduction to NTLM and Netlogon
2. Netlogon vulnerabilities
3. New exploit
History of Windows AD authentication

• 1980’s, early 90’s: LM protocol
  • Password as DES key; very broken

• 1993: NTLMv1
  • MD4 + DES; divide and conquer attack

• 1998: NTLMv2
  • MD4 + HMAC-MD5; relay and offline brute-force issues
    • Enabled by default; hard to get rid off

• 2000: Kerberos (preferred option)
How NTLM works

Session key 🤚 is derived from password hash
How NTLM works

User

Client
password

random challenge

response = MAC(pwd_hash_challenge)

+ MAC(🔒, messages)

challenge + response

Login ok
User: Bob
Groups: ...
Session key: 🔒

Server

Netlogon Remote protocol

DC
The Netlogon Remote protocol

- MSRPC protocol
- Dynamic TCP port (portmapper)
- **Fallback:** tunnel over SMB pipe
- Computer password as shared secret for authentication and crypto
- Message signing/sealing: HMAC-SHA2 + encrypt with AES-CFB8
- Modern client will reject connection if server says it doesn’t support signing/sealing
Prior Netlogon vulnerabilities

• CVE-2015-0005
  • Computer A can submit NTLM handshake intended for computer B
  • Result: steal session key; relay attacks; SMB forgery/decryption...

• CVE-2019-1019
  • Strip computer name from NTLM challenge; client doesn’t mind
  • DC sees no computer name; skips check
  • Same result
The vulnerability

• When client initiates session over TCP and falls back to SMB during a session, it “forgets” about the negotiated encryption method; server accepts this
• Calls still contain “authenticators”, but these do not depend on message content

• Result: MitM can read/change messages!
When you have a MitM position between a domain-joined computer and a DC, and this computer offers some service that accepts NTLM, you can log in as any user, with any password, with any domain privileges.

Made PoC with iptables and Impacket that logs anyone in as Domain Administrator (and thus local admin on the target) with the password “letmein”.
Who is vulnerable

• Typical corporate laptop has SMB service; can get **RCE as local admin** through e.g. the PsExec method

• MitM through e.g. ARP/NDP spoofing, fake Wi-Fi access point, physical access

• Stolen laptop scenario: Bitlocker (TPM Only) bypass
CVE-2019-1424

- Reported to Microsoft
- CVSS score: 8.1
- Recommendation:
  1. Clients should not stop encrypting on SMB fallback
  2. DC’s should not accept unencrypted calls after encryption is negotiated
- Patch released in November 2019
Q&A
Thanks for watching!

Tom Tervoort
tom.tervoort@secura.com