Zerologon Vulnerability

Describing Vulnerabilities

- Common Vulnerability and Exposures (**CVE**)
  - List of publicly disclosed computer security problems
- Common Vulnerability Scoring System (**CVSS**)
  - Numeric score of “how severe” a vulnerability is
  - Ranked from 0-10
    - 0-3.9 : Low
    - 4-6.9 : Medium
    - 7-10.0 : High

Zerologon (CVE-2020-1472)

Zerologon

- **Zerologon**: Unauthenticated domain controller compromise by subverting Netlogon cryptography
  - **CVE-2020-1472**
  - CVSS score: **10.0**
- Discovered and privately reported to Microsoft
  - Patched by Microsoft on August 11 2020
  - Public disclosure Sept 14 2020
    - https://arstechnica.com/information-technology/2020/09/new-windows-exploit-lets-you-instantly-become-admin-have-you-patched/

Attack Requirements

- Attacker needs ability to establish a TCP connection to an unpatched domain controller
  - Typically requires a computer on the local area network (there's no good reason for a domain controller to be internet-accessible)
- No domain credentials are required!
  - Literally plug your laptop into an open Ethernet port…
- Exploits flaws in Microsoft *implementation* of Advanced Encryption Standard (AES)
- Attacker can spoof identity of any computer account (including the domain controller) and set an empty password for that account in the domain

Attack Details

- Netlogon Remote Protocol
  - Allows users to log onto servers using NTLM
  - Lets a computer update its password within a domain
  - Uses a customized cryptographic protocol to allow client to prove to server that it knows a shared secret (and thus is legitimate)

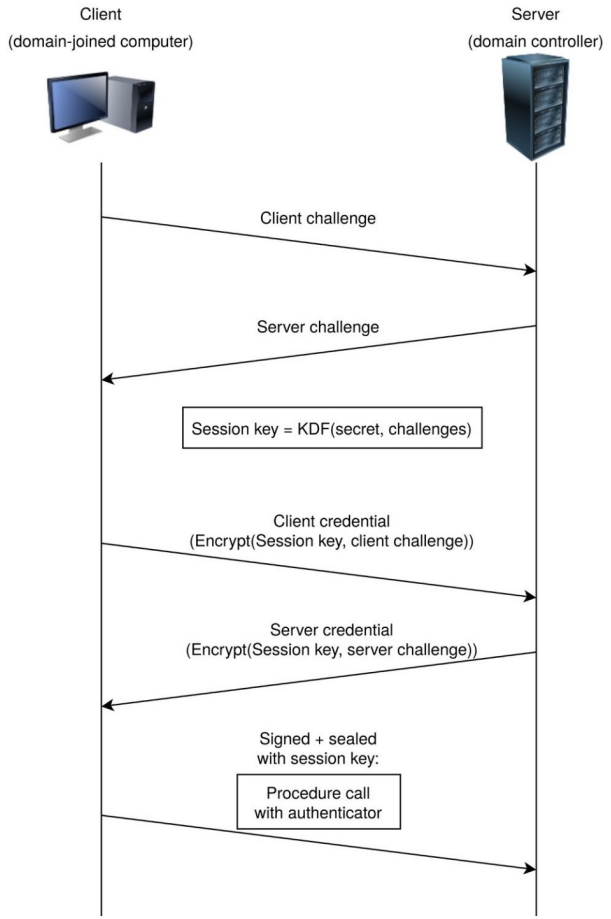


Figure 1: Simplified Netlogon authentication handshake

Attack Details

- Zerologon is an **authentication bypass** attack on the AES cipher
  - Encryption standard requires that the Initialization Vector (IV) is **random**
  - Microsoft implementation used a **fixed** (constant) IV that was 16 zero bytes
- Zerologon tries to authenticate repeatedly with an authentication challenge of 16 zero bytes, and due to <encryption math>, every 1 out of 256 sessions the matching client credential is also 16 zero bytes
  - Identity “confirmed” 😈

Attack Details

- Netlogon normally uses “RPC signing and sealing”
  - Client/attacker can disable this (for backwards compatibility with legacy windows?)
- Netlogon normally uses an authenticator value (based on a timestamp) to prevent replay attacks
  - Client/attacker can provide a time at the beginning of the epoch (Jan 1st, 1970) so the authenticator value is zero
- Now client/attacker can send a Netlogon call as any computer
  - Attacker sets a new computer password for the domain controller

Patch Details

- August 2020 patch from Microsoft now enforces “RPC signing and sealing”, breaking exploit chain
- Additional security update in February 2021 turns on “enforcement mode” (mandating Secure NRPC for all devices)
  - Breaks backwards compatibility with legacy devices

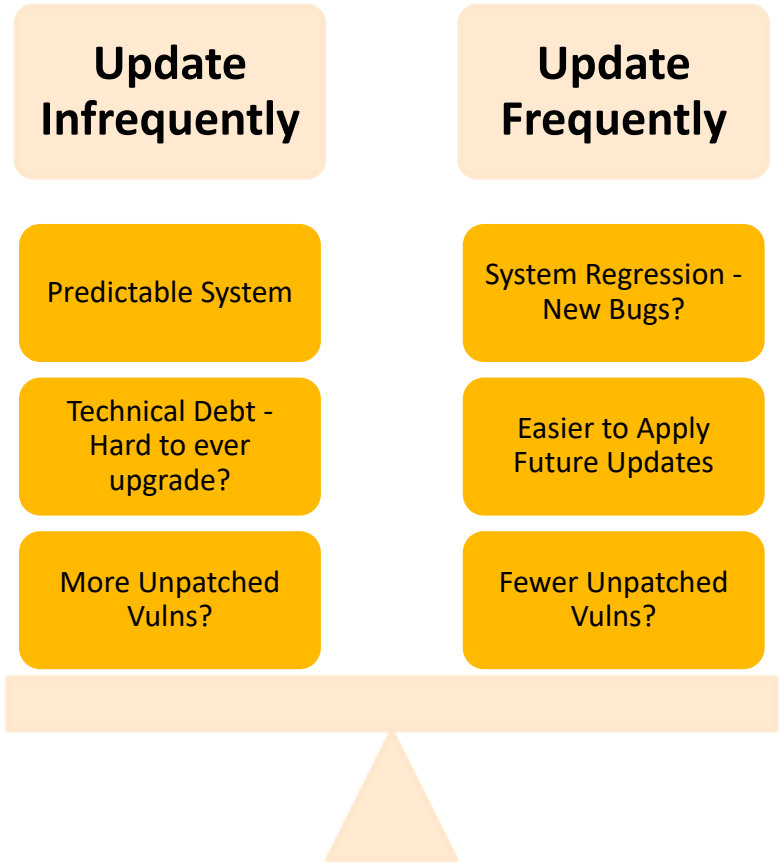
Abusing ZeroLogon – Dump Hashes on Domain Controllers

https://www.youtube.com/watch?v=_HdhhC8UhPA

Zerologon: References

- Blog & Whitepaper from vulnerabilities discoverer
  - https://www.secura.com/blog/zero-logon
- Microsoft security update guide
  - https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
- Python testing script to see if your domain controller is vulnerable
  - https://github.com/SecuraBV/CVE-2020-1472

Applying Updates



Windows Updates

- **Option 1:** Let every user control updates on their own work system
  - *Chaos! Madness! Who knows when users will update?*
- **Option 2:** Microsoft Endpoint Configuration Manager
  - Manages application deployment and software updates (including OS) across a domain
- **Option 3:** Windows Server Updates Services (WSUS)
  - *Caching proxy* for Windows Updates (WSUS downloads updates, administrator *approves* updates for distribution, and endpoints install updates from WSUS proxy)
  - Built into Windows Server
  - Can be mandated by Group Policy!

Active Assignments

- **Project 1**
  - Installation Report – Due Oct 19th
  - Presentation Video – Due Oct 26th
  - Peer Reviews (3) of Video - Due Nov 2nd
- Video
  - 2 minutes – What does app do? Demonstrate that it works
  - 8 minutes – System administration details
    - How to **install** application
    - How to **configure** application
    - How to **secure** application

Active Assignments

- **Lab 9 – Windows Domain Controller** - Due Oct 21st
- **Lab 10 – Windows File Server** - Due Oct 28th
  - Continuation of Domain Controller lab
    - Create a Windows File Server
    - Join it to the domain
    - Demonstrate you have a shared directory
    - Demonstrate that Group Policy can change settings across the domain
    - Demonstrate that the domain controller can remotely access domain computers

Wrap-Up

- Questions?
- Concerns?

- **This Week**
  - **Lab 9 & 10** – Domain Controller and File Server