Security

Exchange Sicherheitslücke CVE-2024-21410 schließen – So geht's!?!

Net at Work
Building IT-Excellence.

Experten für die beste Lösung von allen: Ihre maßgeschneiderte.

Frank
Carius

Enterprise Architect / Partner
MVP | Microsoft Certified Master

Net at Work

Microsoft Solutions Partner
Modern Work

Microsoft Solutions Partner
Security

140+ Mitarbeiter
Gründungsjahr: 1995
Standort: Paderborn

Systemintegrator
mit Lösungen und Werkzeugen für die digitale Kommunikation und Zusammenarbeit

Wir befähigen Menschen durch ein perfektes, digitales Arbeitsumfeld ihre Ziele optimal zu erreichen.

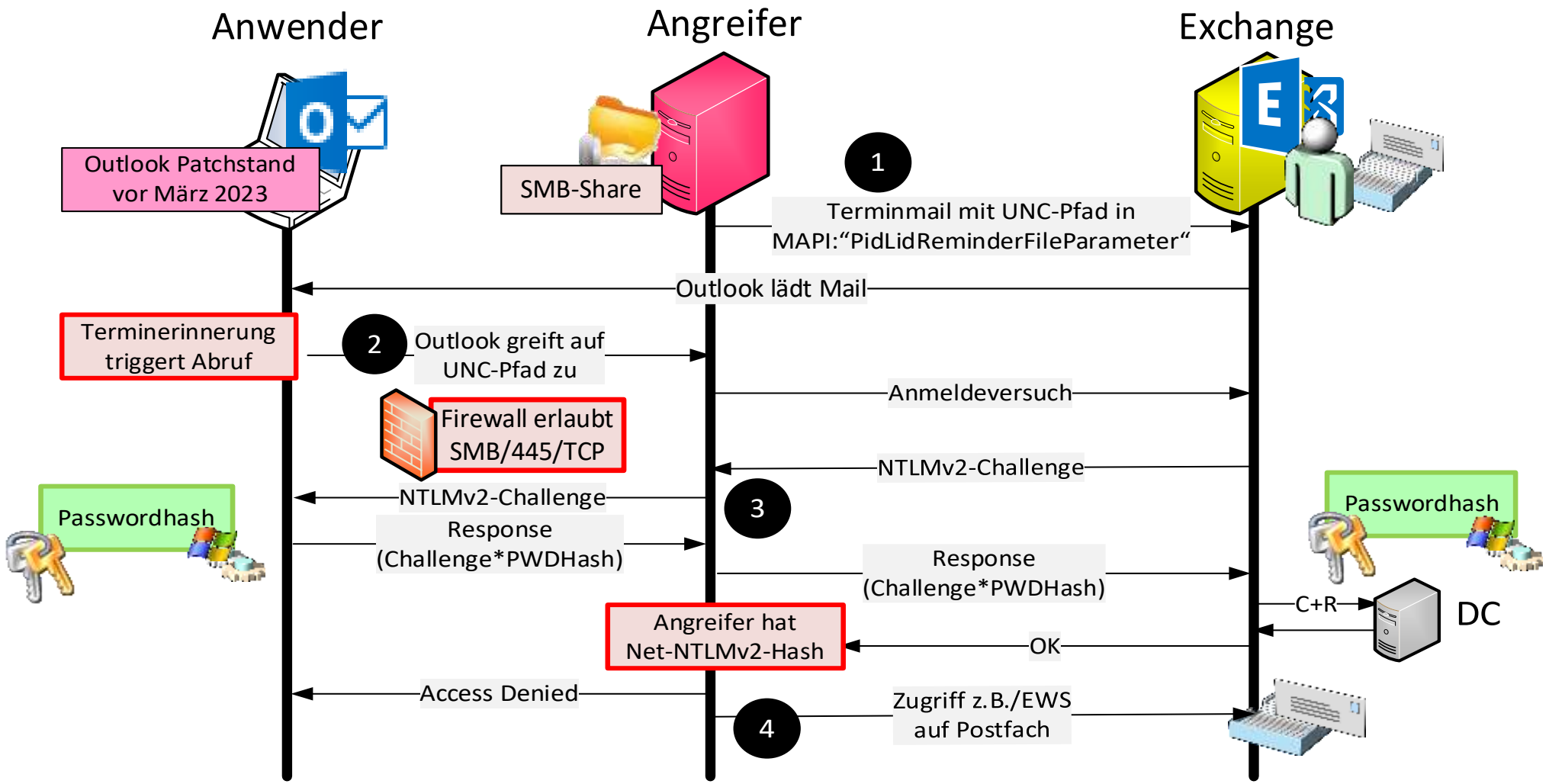
CVE-2024-21410

- Worum geht es bei der Lücke genau?
- Welche Exchange Version ist betroffen?
- Was muss ich tun, um geschützt zu sein?
- Was macht „Extended Protection“ und was muss ich beachten?
- Wie kann ich erkennen, ob ich kompromittiert wurde?

Einordnung der „Priviledge Escalation“

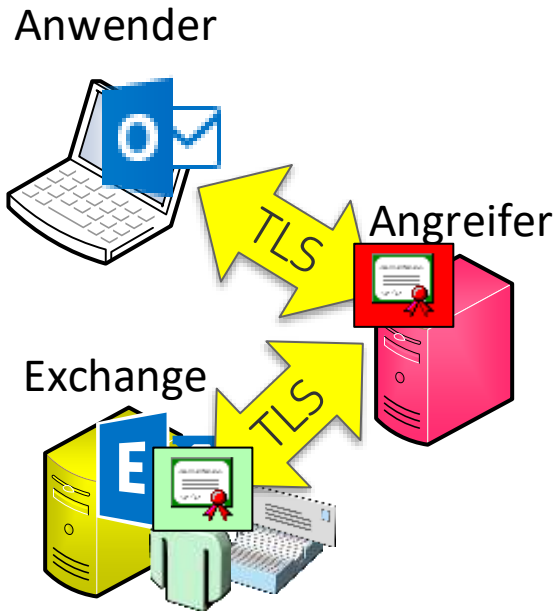
- 13. Feb 2024: CVE-2024-21410 Exchange Server Elevation of Privilege Vulnerability
- 15. Feb 2024: BSI Meldung: Version 1.0: Microsoft Exchange - Aktive Ausnutzung einer Zero-Day-Schwachstelle
  - https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2024/2024-214205-1032.html
- Angreifer können sich „als Benutzer“ am Exchange Postfach anmelden und z.B. …
  - Mails/Kontakte/Termine lesen, schreiben, ändern, Regeln anlegen
- Risiken
  - Abfluss von Informationen
  - Spoofing und Phishing
  - Intern: Angriff auf Admin mit Postfach, um dann z.B. SMB auf C$ zu nutzen?
- Ursache: Outlook und „Windows integrierte Authentifizierung
  - März 2023: (9.8) CVE-2023-23397 Microsoft Outlook Elevation of Privilege Vulnerability (Termineinladung mit UNC-Pfad in “`PidLidReminderFileParameter`”)
  - Feb 2024: (9.8) CVE-2024-21413 Microsoft Outlook Remote Code Execution Vulnerability (Message Preview Exploit öffnet Datei)
  - „Man in the Middle“-Angriffe gegen Outlook und Exchange

Ein möglicher Angriffsvektor: Outlook und Exchange

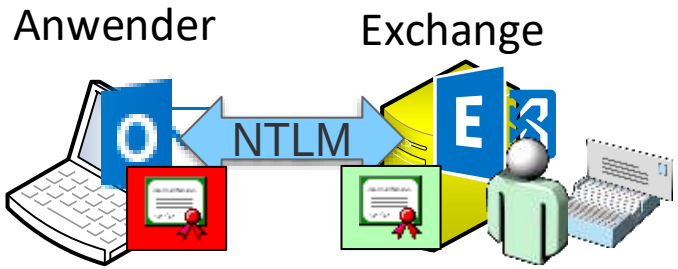


Abhilfe: Extended Protection

- Ohne Extended Protection
  - Client spricht mit Angreifer per TLS verschlüsselt
    Name und Zertifikat bleibt unbemerkt, da Outlook sich im Hintergrund verbindet
  - Angreifer spricht mit Exchange Server
    Exchange kann nicht erkennen, dass es nicht der Anwender ist
  - Man in the Middle (MITM)agiert als Anmelde-Proxy und greift Authentifizierung ab



- Mit Extended Protection
  - TLS-Handshake wird weiter durch Angreifer aufgebrochen
  - Client nutzt das geliefert Zertifikat als Teil der Aufgabe
    - Das Zertifikat kommt vom Angreifer und ist unterschiedlich zum Exchange Server
  - Exchange Server prüft die Antwort zur Ausgabe
    - Nutzt dazu sein eigenes Zertifikat
  - Unterschiedliche Zertifikate verhindern die Anmeldung
    - Fehlerbild: Anwender sehen immer wieder Username/Kennwort-Dialogbox



Extended Protection im Detail

- Feature des IIS
  - Seit IIS 7.5 verfügbar: Windows Vista, Windows 2008
  - Viele Hinweise, die ungehört blieben:
    - Released: August 2022 Exchange Server Security Updates https://techcommunity.microsoft.com/t5/exchange-team-blog/released-august-2022-exchange-server-security-updates/ba-p/3593862
    - Microsoft Security Advisory: Extended protection for authentication https://support.microsoft.com/en-us/topic/microsoft-security-advisory-extended-protection-for-authentication-7dd2ee6d-c2e9-3484-2d8e-466261d3f0c7
    - Microsoft Security Advisory 973811 https://learn.microsoft.com/en-us/security-updates/securityadvisories/2009/973811
- Schützt aber nur „Windows Integrated Authentication“
  - Kein Schutz gegen BasicAuth, Bearer, FormBased etc.
- Auch andere IIS-basierte Dienste (ADFS, SharePoint, 3rd Party)
- EP gibt es auch für andere Protokolle, z.B. LDAPS, TELNET, SMB u.a.
- Achtung bei Layer-7 Loadbalancer und Web Application Firewall
- Achtung bei ausgehenden Proxy-Server mit SSL-Inspection

Andere Gegenmaßnahmen?

- Outlook Updates
  - Sie haben nicht alle Geräte unter Kontrolle und es dauert
  - Die nächste Lücke kommt bestimmt
  - Was ist mit anderen Applikationen, die NTLM machen?
- SMB-Zugriff zum Angreifer unterbinden
  - Ausgehend 445/TCP sollte generell unterbunden sein, auch SMB over QUIC!
  - Homeoffice und Split-VPN
- NTLM-Anmeldung von extern blockieren / Hybrid Modern Auth / OAUTH
  - Nicht möglich, da Kerberos von extern nicht geht (Keine KDC-Verbindung)
  - MRSProxy: Exchange Hybrid Migration braucht NTLM
  - Outlook Client Zugriff (EWS, Free/Busy)
- Indicator of Compromise (IOC):
  - suspekte Login-Vorgänge, Posteingangsregeln, ungewöhnliche Aktivitäten, Source-IPs
  - Vergleichbar zu „User hat sein Kennwort verraten“

Vorarbeiten

- Exchange 2019 CU14 aktiviert „Extended Protection“
  - Andere Exchange Versionen können EP seit Aug 2022!, Kein „neuer“ Code in CU14 als Fix
  - Exchange 2019 CU11/CU12 (+Aug 2022 SU) besser CU13/CU14
  - Exchange 2016 CU22/CU23 (+Aug 2022 SU)
  - Exchange 2013 CU23 (+Aug 2022 SU)
- „Public Folder“ auf Exchange 2016/2019, nicht auf Exchange 2013
- Modern Hybrid Agent
  - „internen“ Server ohne EP in eigener Site bereitstellen
  - Oder „Classic Hybrid“ mit Webveröffentlichung einrichten
- Exchange Veröffentlichung prüfen/anpassen
  - Ggfls. Loadbalancer und Web Application Firewall auf Layer-4 umstellen
  - TLS-Inspection nur mit identischem Zertifikat möglich
  - SSL-Offloading ist nicht erlaubt -> Auf SSL-Bridging umstellen

Extended Protection betreiben

- EP aktivieren (https://aka.ms/ExchangeEPScript)

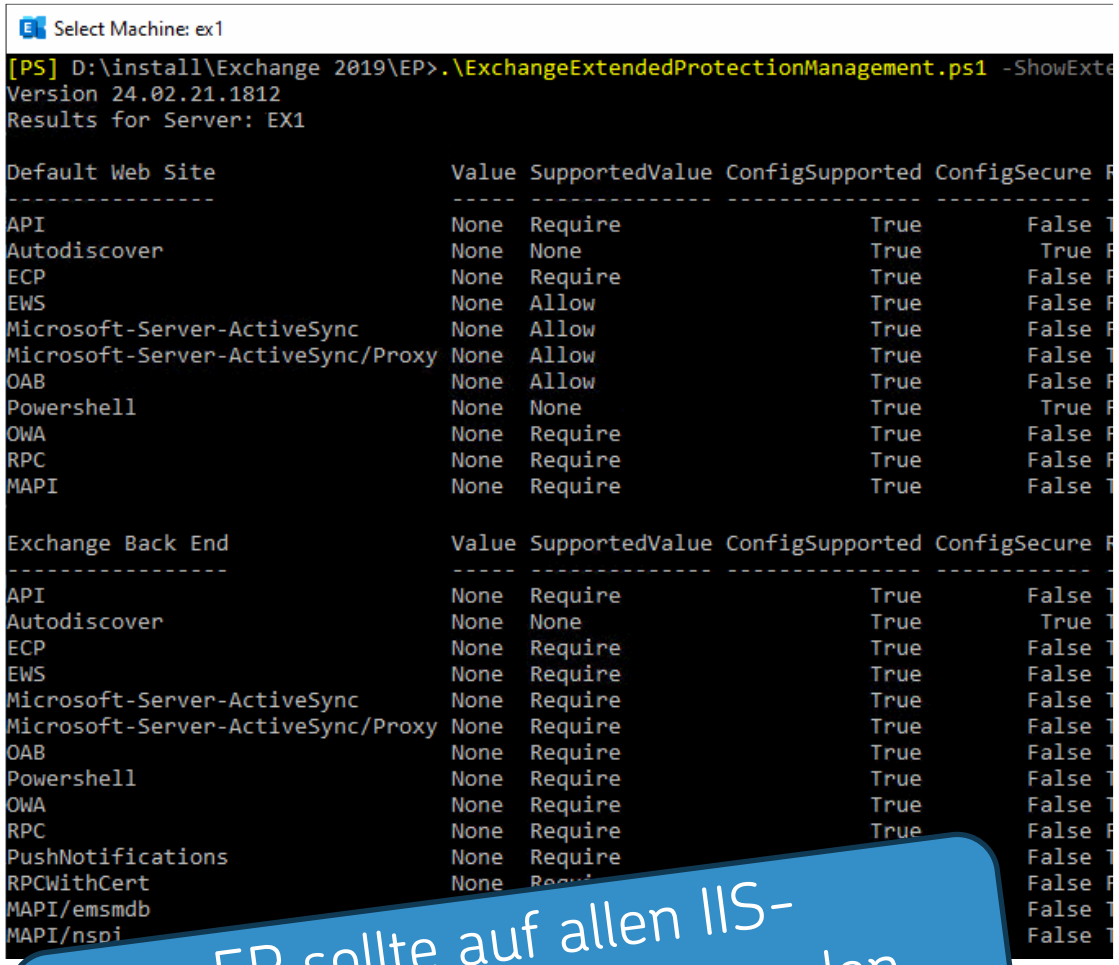
```
PS C:\>
.\ExchangeExtendedProtectionManagement.ps1
-PrerequisitesCheckOnly
PS C:\> .\ExchangeExtendedProtectionManagement.ps1
```

- Im Fehlerfall deaktivieren und fixen

```
PS C:\>
.\ExchangeExtendedProtectionManagement.ps1
-RollbackType "RestoreConfiguration"
```

- Zertifikatswechsel, jedes Jahr aufs Neue
  - Ohne SSL-Mit SSL-Inspection: „Zeitgleich“ auf Exchange und HLB/WAF wechseln
  - Ohne SSL-Inspection: Einfach tauschen
  - Mit SSL-Inspection: „Zeitgleich“ auf Allen wechseln

Configure Windows Extended Protection in Exchange Server
https://learn.microsoft.com/en-us/exchange/plan-and-deploy/post-installation-tasks/security-best-practices/exchange-extended-protection



EP sollte auf allen IIS-Installationen aktiviert werden, nicht nur Exchange!

Vielen Dank für Ihre Aufmerksamkeit.

Net at Work GmbH
Am Hoppenhof 32 A
33104 Paderborn

Kontakt
frank.carius@netatwork.de
https://www.msxfaq.de

Building IT-Excellence.

www.netatwork.de