Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Microsoft Exchange: Aktive Ausnutzung einer Zero-Day-Schwachstelle

CSW-Nr. 2024-214205-1032, Version 1.0, 15.02.2024

IT-Bedrohungslage*: 2 / Gelb

Achtung: Für die schriftliche und mündliche Weitergabe dieses Dokumentes und der darin enthaltenen Informationen gelten gemäß dem Traffic Light Protokoll (TLP) die folgenden Einschränkungen:

TLP:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

Das Dokument ist durch den Empfänger entsprechend den vereinbarten „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten. Weitere Informationen zum TLP finden Sie am Ende dieses Dokumentes.

Sachverhalt

Am 14. Februar 2024 aktualisierte Microsoft sein Advisory zu einer Schwachstelle in Microsoft Exchange Server (CVE-2024-21410), die der Hersteller im Rahmen des Februar Patchdays geschlossen hatte. Ergänzt wurde der Hinweis, dass die Sicherheitslücke bereits aktiv ausgenutzt wird. Die Schwachstelle ermöglicht es externen Angreifenden im Zusammenhang mit potenziellen weiteren Verwundbarkeiten in NTLM-Clients (wie Outlook), sich mit entwendeten Net-NTLMv2-Hashwerten bei einem verwundbaren Exchange Server zu authentifizieren und Aktionen mit den Berechtigungen des ursprünglichen Opfers durchzuführen. Die Bewertung nach dem Common Vulnerability Scoring System (CVSS) in Version 3.1 ist mit einem Wert von 9.8 daher "kritisch".

Diese sogenannten NTLM-Relay-Angriffe können durch die Schutzfunktion Extended Protection (EP), auch Extended Protection for Authentication (EPA) genannt, unterbunden werden, die das Update Exchange Server 2019 CU14 standardmäßig aktiviert.

Betroffen sind Versionen von Microsoft Exchange Server vor Cumulative Update 14 für Exchange Server 2019, ohne aktiviertes Extended-Protection-Feature.

* 1 / Grau: Die IT-Bedrohungslage ist ohne wesentliche Auffälligkeiten auf anhaltend hohem Niveau.
2 / Gelb IT-Bedrohungslage mit verstärkter Beobachtung von Auffälligkeiten unter temporärer Beeinträchtigung des Regelbetriebs.
3 / Orange Die IT-Bedrohungslage ist geschäftskritisch. Massive Beeinträchtigung des Regelbetriebs.
4 / Rot Die IT-Bedrohungslage ist extrem kritisch. Ausfall vieler Dienste, der Regelbetrieb kann nicht aufrecht erhalten werden.

Eine weitere am Februar-Patchday geschlossene kritische Schwachstelle in Outlook (CVE-2024-21413, CVSS-Bewertung ebenfalls 9.8) erlaubt das Entwenden von NTLM-Informationen und möglicherweise auch Codeausführung ohne Nutzerinteraktion bzw. laut Angaben der Entdeckenden der Schwachstelle über einen Klick auf einen präparierten Link in einer Mail [CPR2024]. Microsoft selbst hat die Angabe einer bereits beobachteten Ausnutzung dieser Schwachstelle zurückgezogen und gibt nun an, dass Angriffe unwahrscheinlich seien [MS2024f].

Bewertung

Server mit Microsoft Exchange – und auch Mailserver-Anwendungen im Allgemeinen – dienen in Organisationen als zentrale Knotenpunkte für Kommunikationsflüsse und stellen daher attraktive Ziele für Cyber-Angriffe dar. Eine Kompromittierung kann Tätern dazu dienen, Inhalte auszuspähen, zu sabotieren oder illegitime Mails zu versenden. Ein Ausfall der Anwendungen führt wiederum zu erheblichen Beeinträchtigungen bei betrieblichen Abläufen.

Auch in der Vergangenheit führten Cyber-Angriffe auf Exchange immer wieder zu massiven Schäden in Institutionen.

Im vorliegenden Fall führt die Schwachstelle CVE-2024-21410 in Microsoft Exchange Server in Kombination mit weiteren Sicherheitslücken (wie CVE-2024-21413 in Outlook), die das Entwenden von NTLM-Informationen ermöglichen, zu einem vergleichsweise einfachen Angriffsszenario und sollte entsprechend schnell behoben werden – vor allem, da bereits eine aktive Ausnutzung bekannt ist.

Maßnahmen

IT-Sicherheitsverantwortliche sollten das Sicherheits-Feature Extended Protection (EP) aktivieren, um Exchange Server vor NTLM-Relay-Angriffe zu schützen. Hierzu kann das Cumulative Update 14 for Exchange Server 2019 (KB5035606) installiert werden [MS2024d]. Für ältere Versionen kann EP ebenfalls manuell aktiviert werden.

Microsoft hat EP als optionales Feature für Exchange Server 2013 (End of Support), 2016 und 2019 im Sicherheitsupdate vom August 2022 eingeführt [MS2024b].

Wie EP korrekt konfiguriert wird und was die notwendigen Vorbedingungen sind, kann in der Dokumentation von Microsoft nachgelesen werden [MS2024b]. Mit dem Skript "ExchangeExtendedProtectionManagement.ps1" [MS2024c] ist es möglich, die notwendige Konfiguration vor dem Aktivieren zu prüfen, um daraus folgende Probleme zu verhindern.

IT-Sicherheitsverantwortliche sollten mit dem HealthChecker Tool [MS2024e] abklären, ob auf dem Exchange Server Extendend Protection aktiviert ist/wurde.

Auch wenn Microsoft selbst die Ausnutzung der Schwachstelle CVE-2024-21413 in Microsoft Outlook für unwahrscheinlich hält, sollte sie ebenfalls mit Priorität gepatcht werden [MS2024f]. Eine kurzfristige Prüfung der weiteren Sicherheitshinweise des vergangenen Patchdays wird ebenfalls empfohlen [MS2024g].

Zusätzliche Informationen zur sicheren Konfiguration von Microsoft Exchange und Outlook können dem IT-Grundschutz entnommen werden [BSI2024].

Links

[MS2024a] CVE-2024-21410 - Microsoft Exchange Server Elevation of Privilege Vulnerability:
https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21410

[MS2024b] 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?view=exchserver-2019

[MS2024c] ExchangeExtendedProtectionManagement Tool:
https://microsoft.github.io/CSS-Exchange/Security/ExchangeExtendedProtectionManagement/

[MS2024d] Cumulative Update 14 for Exchange Server 2019 (KB5035606):
https://support.microsoft.com/de-de/topic/kumulatives-update-14-f%C3%BCr-exchange-server-2019-kb5035606-5d08ad6d-3527-41c9-82b6-e19d3ddf94db

[MS2024e] HealthChecker Tool:

https://microsoft.github.io/CSS-Exchange/Diagnostics/HealthChecker/

[MS2024f] CVE-2024-21413 - Microsoft Outlook Remote Code Execution Vulnerability:
https://msrc.microsoft.com/update-guide/en-US/advisory/CVE-2024-21413

[MS2024g] February 2024 Security Updates:
https://msrc.microsoft.com/update-guide/releaseNote/2024-Feb

[CPR2024] The Risks of the #MonikerLink Bug in Microsoft Outlook and the Big Picture:
https://research.checkpoint.com/2024/the-risks-of-the-monikerlink-bug-in-microsoft-outlook-and-the-big-picture/

[BSI2024] BSI IT-Grundschutz: APP.5.2 Microsoft Exchange und Outlook:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_5_2_Microsoft_Exchange_und_Outlook_Edition_2023.pdf

Anlagen

Kontakt

Bitte wenden Sie sich bei allen Rückfragen zu diesem Dokument an denjenigen Kontakt, der Ihnen das Dokument zugesendet hat. Dadurch bleibt der Informationsfluss kanalisiert. Die Single Points of Contact (SPOCs), welche das Dokument direkt vom Nationalen IT-Lagezentrum des BSI erhalten haben, können sich direkt an die bekannten Kontaktdaten des Nationalen IT-Lagezentrums im BSI wenden.

Erklärungen zum Traffic Light Protokoll (TLP)

Dieses Dokument und die darin enthaltenen Informationen sind gemäß dem TLP eingestuft:

1) Was ist das Traffic Light Protokoll?

Das vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.

2) Welche Einstufungen existieren?

- **TLP:CLEAR: Unbegrenzte Weitergabe**
  Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.

- **TLP:GREEN: Organisationsübergreifende Weitergabe**
  Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.

- **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
  Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

    TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe
    Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.

- **TLP:RED: Persönlich, nur für benannte Empfänger**
  Informationen dieser Stufe sind auf den Kreis der Anwesenden in einer Besprechung oder Video-/Audiokonferenz bzw. auf die direkten Empfänger bei schriftlicher Korrespondenz beschränkt. Eine Weitergabe ist untersagt. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.

3) Was mache ich, wenn ich das Dokument an jemanden außerhalb des im TLP vorgegebenen Informationsverbundes weitergeben will?

Sollte eine Weitergabe an einen nicht durch die Einstufung genehmigten Empfängerkreis notwendig werden, so ist diese vor einer eventuellen Weitergabe durch den Informationsersteller nachvollziehbar zu genehmigen. Bei ausnahmsweiser Weitergabe im Rahmen einer bestehenden gesetzlichen Verpflichtung ist der Informationsersteller – nach Möglichkeit vorab – zu informieren.

4) Was passiert, wenn ich die Einstufung nicht beachte?

Bei Verstoß gegen die Regeln zur Weitergabe von Informationen erhält der Verpflichtete zukünftig nur noch TLP:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.