HAFNIUM – HILFE ZUR SELBSTHILFE

Erste Schritte zur Behandlung der Sicherheitslücken im Microsoft Exchange Server

Stand: Version 1.6, 24.03.2021, 01:00

SACHVERHALT

Microsoft hat am 3. März 2021 sogenannte “Out-of-Band”-Updates für Exchange Server veröffentlicht. “Out of Band” bedeutet, dass die Patches von Microsoft als wichtig angesehen und sofort installiert werden sollten. Mit dem Update werden vier kritische Schwachstellen geschlossen, die bereits für Angriffe verwendet werden, und die Angreifern die Möglichkeit bieten, vertrauliche Daten abzugreifen oder Schadsoftware zu installieren.

HINWEIS: Im Folgenden werden die aktuell verfügbaren Informationen genutzt, um eine mögliche Vorgehensweise zu definieren. Das Dokument wird laufend aktualisiert. Bitte achten Sie daher auch auf weitere Veröffentlichungen unter

https://research.hisolutions.com/

BETROFFENE SYSTEME

Laut den Hinweisen des Herstellers[1] sind die folgenden Systeme betroffen:

- Exchange 2010 (nur Schwachstelle CVE-2021-26857)
- Exchange 2013
- Exchange 2016
- Exchange 2019

Sofern Sie Exchange 2003 oder 2007 einsetzen sollten, sind Sie vermutlich nicht betroffen. Der Support dieser Systeme ist jedoch abgekündigt und diese weisen andere kritische Schwachstellen auf und sollten deshalb sofort auf eine aktuelle Version aktualisiert werden!

Der Cloud-Dienst Exchange Online ist NICHT betroffen.

[1] https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

TLP:WHITE

HISOLUTIONS

HiSolutions AG
Schloßstraße 1
12163 Berlin

info@hisolutions.com
www.hisolutions.com

+49 30 533 289-0
+49 30 533 289-900

SCHRITTE ZUR BEHANDLUNG DER SCHWACHSTELLE

Schritt 1: Verhindern weiterer Angriffe

HINWEIS: Die folgenden Schritte beinhalten Maßnahmen, welche von technisch versiertem Personal durchgeführt werden sollten. Bitte geben Sie dieses Dokument im Zweifel an Ihren IT-Dienstleister, welcher zusammen mit Ihnen diese Schritte abarbeiten kann.

Da die Schwachstelle aktiv ausgenutzt wird, empfehlen wir vor der Suche nach möglichen Kompromittierungen die folgenden Schritte, um eine akute Infektion zu verhindern:

- Falls noch nicht geschehen: Sofortiges Installieren der von Microsoft veröffentlichten Sicherheitsupdates. Sofort bedeutet hierbei innerhalb der nächsten 2 Stunden, nachdem Sie diese Information erhalten haben.
    - Sofern eine Aktualisierung mittels des von Microsoft bereitgestellten Sicherheitsupdates nicht möglich ist, sollten die folgenden von Microsoft empfohlenen Maßnahmen durchgeführt werden[2]
        - Deaktivieren von Unified Messaging (UM)
        - Deaktivieren von Exchange Control Panel (ECP) VDir
        - Deaktivieren des Offline Address Book (OAB) VDir
        - Deaktivieren von Active Sync
        - Deaktivieren des Outlook Web Access Zugang
- Zusätzlich wird die sofortige Sperrung von Port 443 an der Firewall bzw. die Trennung des Exchange-Servers vom Internet bis zum Einspielen der Patches empfohlen, sofern diese Maßnahme möglich ist und die Installation der Sicherheitsaktualisierungen nicht verzögert wird.

HINWEIS: Wir raten Ihnen dringend an, eine Meldung eines Datenschutzvorfalls zu prüfen. Je nach Bundesland gibt es hierzu unterschiedliche Auslegungen[3].

Schritt 2: Überprüfen einer möglichen Kompromittierung

Um eine mögliche Kompromittierung Ihrer Systeme überprüfen zu können, befolgen Sie bitte die folgenden Schritte:

1. Sichern der folgenden Daten für eine spätere Analyse, sofern diese notwendig sein sollte, z. B. durch Vollsicherung oder Snapshot (inkl. Memory) des Exchange Systems.
    - Exchange Server
        - Protokolldateien des IIS-Servers unter C:\inetpub\Logs\
        - Protokolldateien des Exchange-Server unter <Exchange_Instalationspfad>\v15\Logging\ (mind. ab dem 24.02.)
        - Inhalt des Ordners inetpub

[2] https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
[3] https://www.reuschlaw.de/news/hafnium-schwachstellen-bei-exchange-melde-und-benachrichtigungspflichten-nach-der-dsgvo/

- Sämtliche Windows Event Logs (C:\Windows\System32\winevt\logs\)

o Domänen-Controller
  Sämtliche Windows Event Logs (C:\Windows\System32\winevt\logs\)

2. Durchführen einer Offline-Sicherung (z. B. auf eine externe Festplatte) von Systemsicherungen (Exchange und Domäne vom letzten Sicherungsstand vor dem 02.03.2021)

3. Ausführen des Microsoft-Prüfskriptes[4] (Test-ProxyLogon.ps1 und CompareExchangeHashes.ps1). Bitte folgen Sie der dortigen Anleitung.

   Als Ergebnis erhalten Sie eine CSV Datei, die Sie selber analysieren können.

	H	I
	AnchorMailbox	HttpStatus
	ServerInfo~a]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~a]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~akak]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~akak]@contoso.com:444/mapi/emsmdb/?#	200
	ServerInfo~akak]@contoso.com:444/ecp/proxyLogon.ecp?#	241
N1	ServerInfo~a]@contoso.com:444/autodiscover/autodiscover.xml?#	200
	ServerInfo~a]@contoso.com:444/mapi/emsmdb/?#	200
	ServerInfo~a]@contoso.com:444/ecp/proxyLogon.ecp?#	241

Abbildung 1 Mögliches Ergebnis des Microsoft-Prüfskriptes[3]

HINWEIS: Für Organisationen, die keine Möglichkeit haben einen Incident Response Dienstleister in Anspruch zu nehmen, hat Microsoft ein automatisiertes Tool zur Prüfung betroffener Systeme veröffentlicht[5]. Das Tool setzt Sofortmaßnahmen direkt um und versucht Änderungen an den Systemen durch Angreifer wieder rückgängig zu machen. Derzeit liegen uns keine Erfahrungswerte zur Zuverlässigkeit des neuen Werkzeugs vor.

Option 1: Vermutlich KEINE Kompromittierung
Sofern Sie keine Einträge sehen oder nur Einträge mit der Endung

```
444/autodiscover/autodiscover.xml?#","200"
```

gehen wir und Microsoft[6] aktuell davon aus, dass keine erfolgreiche Kompromittierung stattgefunden hat. Die Meldung ist ein Indiz dafür, dass eine der veröffentlichten Schwachstellen ausgenutzt werden sollte, der Angreifer jedoch keine valide E-Mail-Adresse gefunden hat. In diesem Fall können Sie prüfen, ob Sie die unter „Vorbeugende Maßnahmen“ aufgeführten Punkte umsetzen werden.

[4] https://github.com/microsoft/CSS-Exchange/tree/main/Security
[5] https://msrc-blog.microsoft.com/2021/03/15/one-click-microsoft-exchange-on-premises-mitigation-tool-march-2021/
[6] https://github.com/microsoft/CSS-Exchange/commit/19778cd80c98b5c395079ef9d1f3ac1d1b059a40

Option 2: Vermutlich eine Kompromittierung
Sofern Sie andere Einträge finden, wie beispielweise

```
444/mapi/emsmdb/?#","200"
444/ecp/proxyLogon.ecp?#","241"
```

gehen wir von einer Kompromittierung des Systems aus. Sollte dies der Fall sein, sollten Sie die Maßnahmen unter „Schritt 3: Maßnahmenempfehlungen (bei Kompromittierungsverdacht)“ umzusetzen.

HINWEIS: Es wurde ein Zugriff auf das IT-System Exchange mittels einer Schwachstelle festgestellt. Damit war dem Angreifer grundsätzlich ein Zugriff auf personenbezogene Daten möglich, dieser ist mit den bisherigen Ergebnissen noch nicht validiert. Bitte prüfen Sie daher zusammen mit ihrem Datenschutzbeauftragten, ob eine Meldung nach DSGVO im Rahmen der Frist von 72 Stunden abgegeben werden sollte!

4. Nutzung des Thor-Lite Scanner[7]. Eine Anleitung zur Nutzung haben wir in unserem Research Blog[8] veröffentlicht.

HINWEIS: In älteren Versionen dieses Dokumentes haben wir die Nutzung des Microsoft Support Emergency Response Tool[9] (MSERT) empfohlen. Obwohl dieses Werkzeug zweckmäßig ist, raten wir zur Vorsicht bei dessen Nutzung. MSERT löscht u. U. Shells und kann die vollständige Bereinigung nicht sicherstellen. Wir empfehlen die Nutzung mit der Option /N und der Sicherung der gefundenen Dateien. Hierbei werden die Daten nicht gelöscht und können von einem Spezialisten im Anschluss noch untersucht werden.

Schritt 3: Maßnahmenempfehlungen (bei Kompromittierungsverdacht)

Es ist bislang noch nicht bekannt, zu welchem Zweck die Server angegriffen werden. Die Anzahl der Angreifergruppen hat sich seit der Veröffentlichung stark vergrößert. Aus diesem Grund lässt sich aktuell nicht abschätzen, welche Maßnahmen ausreichend sind, um die Systeme zu bereinigen.

Als ersten Schritt sollten Sie überprüfen, ob die Angreifer zusätzlich zu den automatischen Angriffen und dem möglichen Abgriff von Adressbüchern und E-Mails weitere Angriffe durchgeführt haben. Hierzu wird auf die Existenz von sogenannten „Webshells“ geprüft.

Die Schwachstelle wird bereits durch mehrere Gruppen ausgenutzt, sodass eine Suche nach Webshells der Ursprungsgruppe nicht ausreichend ist. Das BSI hat eine Übersicht Im Dokument „Microsoft Exchange Schwachstellen Detektion und Reaktion“[10] über mögliche Wege zur Suche nach Webshells veröffentlicht.

[7] https://www.nextron-systems.com/thor-lite/
[8] https://research.hisolutions.com/
[9] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
[10] https://bsi.bund.de/exchange-schwachstellen

Bitte prüfen Sie die folgenden Verzeichnisse (inkl. Unterverzeichnisse) auf zuletzt veränderte bzw. erstellte ASPX-Dateien (im letzten Monat), oder ASPX-Dateien, welche dem Benutzer „NT AUTHORITY\SYSTEM“ gehören.

- C:\inetpub\wwwroot\aspnet_client\
- <Exchange Installationspfad>\V15\FrontEnd\HttpProxy\owa\auth\
- C:\Exchange\FrontEnd\HttpProxy\owa\auth\

HINWEIS: Es handelt es sich bei den angegebenen Pfaden um Beispielpfade. Die exakten Pfade können sich je nach Installationsort und Exchange-Version unterscheiden.

Zudem können Sie den Thor-Lite Scanner[7] nutzen, um nach möglichen Webshells zu suchen. Eine Anleitung zur Nutzung haben wir in unserem Research Blog[11] veröffentlicht. Das bisher von uns empfohlene Detektions-Skript des lettischen CERT[12] wird NICHT weiter gepfegt. Wir raten daher von der weiteren Anwendung ab.

Im Internet finden Sie ebenfalls eine umfangreiche Liste[13] mit möglichen Namen für Webshells.

HINWEIS: Aufgrund der Vielzahl von möglichen Angreifern kann dies nur als ein Indiz gesehen werden. Wiederholen Sie die Prüfung regelmäßig mit aktualisierten Signaturen.

HINWEIS: Das vermutliche Kompromitierungsdatum berechnet sich aus dem ersten auftreten einer Webshell auf Ihren Systemen. Sofern Sie durch einen Fallbetreuer bei der HiSolutions unterstützt werden, kann dieser Ihnen bei der Einschätzung helfen.

Option 1: Es wurde KEINE Web-Shell gefunden

Sensibilisieren Sie ihr Personal sowie Ihre Kooperationspartner, Kunden und Dienstleister in Bezug auf mögliche Phishing-Angriffe in Bezug auf aktuelle Vorgänge und Abläufe.

Führen Sie eine vollständige Virenprüfung Ihrer IT-Systeme durch (z. B. durch Microsofts Security Scanner MSERT[9]).

HINWEIS: In älteren Versionen dieses Dokumentes haben wir die Nutzung des Microsoft Support Emergency Response Tool[14] (MSERT) empfohlen. Obwohl dieses Werkzeug zweckmäßig ist, raten wir aktuell zur Vorsicht bei der Nutzung von MSERT. Es löscht u. U. Shells und kann die vollständige Bereinigung nicht sicherstellen. Wir empfehlen die Nutzung mit der Option /N und der Sicherung der gefundenen Dateien. Hierbei werden die Daten nicht gelöscht und können von einem Spezialisten im Anschluss noch untersucht werden. Während des Scans können Dateien als infiziert angezeigt werden. Diese werden im ersten Schritt jedoch nur als „auffällig markiert" und werden bei einem möglichen Internetzugriff in der Microsoft-Cloud nochmal analysiert. Wenn das negativ ausfällt, wird die Markierung entfernt und der Safety Scanner zeigt im Zweifelsfall als Endergebnis keine Befunde, obwohl während des Scans tatsächlich Befunde vorlagen.

[11] https://research.hisolutions.com/
[12] https://github.com/cert-lv/exchange_webshell_detection
[13] https://gist.github.com/JohnHammond/0b4a45cad4f4ed3324939d72dc599883
[14] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download

Es wird empfohlen, ein Backup des betroffenen Exchange-Servers wiederherzustellen (Backup vor dem 02.03.2021 bzw. vor dem bei Ihnen festgestellten Kompromittierungsdatum).

Vergewissern Sie sich, dass Sie die folgenden Schritte durchgeführt haben:

- Einspielen aller von Microsoft zur Verfügung gestellten Patches
- Systematisches Ändern von Zugangsdaten und Passwörtern, insbesondere bei administrativen Benutzerkonten
- Zurücksetzen des Computer-Kontos für den Exchange-Server[15]
- Umsetzen der Maßnahmen im Kapitel **„**Vorbeugende Maßnahmen**“**

Option 2: Es wurde eine Web-Shell gefunden

Dies kann ein Indiz für eine tiefere Kompromittierung sein. Gemäß den BSI-Empfehlungen[10] sollte Ihre Organisation in den Incident-Response-Modus übergehen.

Stellen Sie ein Backup des betroffenen Exchange-Servers her (Backup vor dem 2.3.2021 bzw. vor dem bei Ihnen festgestellten Kompromittierungsdatum). Das System muss dabei zunächst vom Internet getrennt sein. Ein Zugriff auf die Domäne ist legitim, sofern notwendig.

Eine Eingrenzung des Angriffes ist aktuell nicht möglich. Daher haben Sie folgenden Optionen:

- **Umzug des Exchange in die Cloud**: Hierbei lassen sich die Maildatenbanken in die Cloud migrieren. Das Azure AD und der Exchange Online werden durch Microsoft betrieben. Die Umstellung sollte gut geplant sein und birgt Risiken (Umstellung der Benutzer im Home Office, kurzfristiger Ausfall der Infrastruktur). Zudem kann nicht ausgeschlossen werden, dass der Angreifer trotzdem noch im System ist.
- **Nutzung eines spezialisierten Diensleisters:** Sofern Sie Ihren Exchange Server selber betreuen, sollten Sie überprüfen, ob eine Auslagerung zu einem spezialisierten Dienstleister sinnvoll ist. Dieser übernimmt die Wartung und Pflege und sollte auch die Absicherung des Systems übernehmen.
- **Active Directory Domain Compromise**: Sollte man davon ausgehen, dass das Active Directory kompromittiert ist, bleiben nur zwei Optionen: Das vollständige Neuaufsetzen des AD oder ein Rettungsversuch mittels Golden-Ticket Mitigation, Neuvergabe sämtlicher Credentials (inkl. Service Accounts) und Verifizierung sämtlicher Accounts, Gruppen und Berechtigungen im AD. Es empfiehlt sich, einen solchen Rettungsversuch von einem Incident Response Dienstleister begleiten zu lassen, es handelt sich um einen sehr komplexen Vorgang.
- **Exchange neu aufsetzen bzw. aus Backup zurück spielen (Disaster Recovery)**:
    - Exportieren der Postfächer und Außerbetriebnahme des Altsystems
    - Wiederherstellung der Exchange-Server: Wenn Sie über ein nicht-kompromittiertes Backup verfügen (Backup vor dem 2.3.2021 bzw. vor dem bei Ihnen festgestellten Kompromittierungsdatum), können Sie das System aus diesem Backup wiederherstellen, alternativ können Sie ein neues Exchange aufsetzen.

[15] https://docs.microsoft.com/de-de/troubleshoot/windows-server/windows-security/use-netdom-reset-domain-controller-password

  - Achten Sie darauf, den Exchange-Server nicht online (von außen zugänglich) zu machen, bevor Sie die untenstehenden Maßnahmen durchgeführt haben. Dieser darf nur wieder online gehen, wenn alle Patche installiert worden sind.
  - Zur Wiederherstellung durch Neuinstallation gibt es eine Anleitung von Microsoft zum Exchange Disaster Recovery[16].
  - Zur Wiederherstellung des Exchange Servers aus dem Backup sollten Sie sicherstellen, dass die Sicherung vor dem Eintritt des Schadens durchgeführt wurde; prüfen Sie das Backup auch mit dem von Microsoft bereitgestelltem Skript. Prüfen Sie auf ein Update des Skriptes.
  - Spielen Sie die gesicherten Postfächer zurück und binden Sie diese neu ein.
- **Untersuchung der Umgebung durch einen Incident Responder**: Hierbei wird die Umgebung auf mögliche versteckte Angreifer untersucht. Diese Untersuchung kann sich über mehrere Wochen ziehen. Im Normalfall wird bei einer Kompromittierung eine komplette Neuinstalltion der Umgebung empfohlen.

Die folgenden zusätzlichen Maßnahmen innerhalb Ihrer Windows-Domäne sollten Sie ebenfalls zur Vorbeugung durchführen:

- Wechsel der Passwörter aller administrativen Konten
- Zurücksetzen des Computer-Kontos für den Exchange-Server[15]
- Invalidieren von Golden-Ticket-Angriffen durch doppelte Passwortänderung des KRBTGT-Benutzerkontos[17] [18]
- Überprüfen auf neu angelegte Benutzerkonten im Active Directory während des Kompromittierungszeitraums mit Schwerpunkt auf administrativen Konten
- Prüfen Sie die folgenden Gruppenmitgliedschaften im Active Directory auf neue oder geänderte Accounts:
  - "Exchange Organization Administrators"
  - "Exchange Windows Permissions"

[16] https://docs.microsoft.com/en-us/exchange/high-availability/disaster-recovery/recover-exchange-servers?view=exchserver-2019
[17] https://cert.europa.eu/static/WhitePapers/CERT-EU-SWP_14_07_PassTheGolden_Ticket_v1_1.pdf
[18] http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf

Vorbeugende Maßnahmen

Bei einer Kompromittierung ist es auf jeden Fall ratsam, dass die folgenden Maßnahmen durchgeführt werden, um mögliche Folgeangriffe zu erkennen oder gar zu verhindern:

- Erhöhen der Protokollierung
  - Erhöhen Sie die Mindestaufbewahrungsfrist der Logfiles bei ausreichend freiem Speicher auf folgenden IT-Systemen:
    - Security Log des Domänenkontrollers
    - Exchange-Zugriffsprotokolle
    - Web Proxy-Log
    - Firewall-Logs
  - Überprüfen der Logfiles auf besonders relevanter Ereignismeldungen
    - Hierbei können die SIGMA Regeln[19] verwendet werden, um die Logfiles automatisiert zu überwachen
    - Überwachen Sie externe erreichbare Fernzugänge ohne Mehr-Faktor-Authentifizierung auf unbefugte Zugriffe
- Wöchentliches Überprüfen der Server mittels des Microsoft Safety Scanners[20]
- Nutzung des Thor-Lite[7] Scanners. Eine Anleitung zur Nutzung haben wir in unserem Research Blog veröffentlicht.
- Systematisches Ändern von Zugangsdaten und Passwörtern, insbesondere bei administrativen Benutzerkonten
- Überprüfen des Exchange Servers auf neu angelegte Benutzerkonten, Dienste oder zusätzlich ausgeführte Programme bzw. abgelegte Dateien
- Führen Sie regelmäßig eine vollständige Virenprüfung Ihrer IT-Systeme durch
- Erwägen Sie die Einführung einer Mehr-Faktor-Authentifizierung für externe Zugänge zu Ihrem Netzwerk
- Sofern noch nicht vorhanden, führen Sie eine Offline-Datensicherung ein
- Sensibilisierung von Personal und Dienstleistern im Hinblick auf mögliche Phishing-Angriffe/CEO-Fraud-Szenarien. Warnen Sie insbesondere vor E-Mails, die mit Bezug auf bestehende E-Mails auf geänderte Bankverbindungen oder Lieferadressen hinweisen bzw. ungewöhnliche Anlagen enthalten. Hilfestellung zum Erkennen von verdächtigen E-Mails stellt das BSI auf seiner Website[21] bereit.

Wir empfehlen die Beobachtung der Systeme gemäß diesen Empfehlungen für einen Zeitraum von 12 Monaten. In der Vergangenheit haben wir häufig 'Ruhezeiten' (nach initialer Kompromittierung bis zum eigentlichen Angriff) von 2-4 Monaten, in einigen Fällen aber auch bis zu 9 Monaten gesehen.

Prüfen Sie in der nächsten Zeit regelmäßig die folgenden Seiten auf neue Hinweise:

- https://research.hisolutions.com/hafnium
- https://bsi.bund.de/exchange-schwachstellen

[19] https://github.com/SigmaHQ/sigma/tree/master/rules/windows/builtin
[20] https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/safety-scanner-download
[21] https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/spam-phishing-co_node.html