Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Mehrere Schwachstellen in MS Exchange

CSW-Nr. 2021-197772-14F2, Version 1.4, 06.03.2021

IT-Bedrohungslage*: 4 / Rot

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:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE 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

In der Nacht zum Mittwoch, den 3. März 2021, hat Microsoft Out-of-band Updates für Exchange Server veröffentlicht. Hiermit werden vier Schwachstellen geschlossen, die in Kombination bereits für zielgerichtete Angriffe verwendet werden und Tätern die Möglichkeit bieten, Daten abzugreifen oder weitere Schadsoftware zu installieren.

Bei den Schwachstellen handelt es sich um:

- CVE-2021-26855 ist eine server-side request forgery (SSRF) Schwachstelle in Exchange, welche es einem Angreifer erlaubt, HTTP-Requests zu senden und sich am Exchange-Server zu authentisieren.
- CVE-2021-26857 ist eine insecure deserialization Schwachstelle im Unified Messaging Service. Bei insecure deserialization werden nutzer-bestimmte Daten von einem Programm deserialisiert. Hierüber ist es möglich, beliebigen Programmcode als SYSTEM auf dem Exchange-Server auszuführen. Dies erfordert Administrator-Rechte oder die Ausnutzung einer entsprechenden weiteren Schwachstelle.
- CVE-2021-26858 und CVE-2021-27065 sind Schwachstellen, mit denen – nach Authentisierung – beliebige Dateien auf dem Exchange-Server geschrieben werden können. Die Authentisierung kann z. B. über CVE-2021-26855 oder abgeflossene Administrator-Zugangsdaten erfolgen.

* 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.

Nach Angaben des Herstellers richteten sich die Angriffe gegen amerikanische Forschungseinrichtungen mit Pandemie-Fokus, Hochschulen, Anwaltsfirmen, Organisationen aus dem Rüstungssektor, Think Tanks und NGOs. Microsoft vermutet hinter den Vorfällen eine staatliche Hackergruppe aus China, die HAFNIUM genannt wird.

Namen der Opfer sind im BSI nicht bekannt. Bei den beobachteten Angriffen wurde hierüber Zugang zu den E-Mail-Accounts erlangt sowie weitere Malware zur Langzeit-Persistenz installiert [MIC2021a].

Die Attacken erfordern die Möglichkeit, eine nicht-vertrauenswürdige Verbindung auf Port 443 zu dem Exchange-Server zu etablieren. Daher sind Server geschützt, welche nicht-vertrauenswürdige Verbindungen beschränken oder nur per VPN erreichbar sind. Diese Lösung schützt allerdings nur vor dem initialen Angriff, andere Teile können genutzt werden, wenn ein Angreifer bereits Zugriff auf den Server hat oder ein Administrator eine schadhafte Datei ausführt [MIC2021b].

Sicherheitsupdates stehen für die folgenden Versionen zur Verfügung [MIC2021c]:

- Exchange Server 2010 (RU 31 für Service Pack 3, hierüber werden künftige Angriffe verhindert)
- Exchange Server 2013 (CU 23)
- Exchange Server 2016 (CU 19, CU 18)
- Exchange Server 2019 (CU 8, CU 7)

Nicht betroffen ist Exchange Online [MIC2021c].

Update 1:
Aufgrund der großen Wahrscheinlichkeit einer Ausnutzung und dem damit verbundenen Risiko wurde von der amerikanischen Cybersecurity and Infrastructure Security Agency (CISA) noch am Dienstag eine Emergency Directive erlassen [CIS2021a]. Darin werden die US-Bundesbehörden angewiesen, anfällige Exchange-Server zu identifizieren, auf entsprechenden Systemen nach den unter [CIS2021b] veröffentlichten Angriffsindikatoren zu suchen und diese bei Auffälligkeiten einer genauen forensischen Analyse zu unterziehen.

Weiterhin weist Rapid 7 in seinem Blog auf eine hohe Zahl bedrohter Systeme in Deutschland hin [RAP2021].

Update 2:
Das **Risiko erfolgreicher Angriffe** besteht insbesondere **für alle aus dem Internet erreichbaren Exchange-Server** (z. B. im Falle einer Erreichbarkeit via **Outlook Web Access** (OWA)), wenn die Verbindung nicht ausschließlich mittels VPN erfolgt.

Laut der Server-Suchmaschine Shodan betrifft die Schwachstelle potentiell etwa 57000 Server in Deutschland [TWI2021b].

Update 3:
Die Verwundbarkeit über nicht-vertrauenswürdige Verbindungen auf Port 443 kann grundsätzlich durch jeden Exchange Web Dienst verursacht werden, d. h. nicht nur durch OWA, sondern auch bei der Nutzung von **ActiveSync,Unified Messaging (UM)**, dem **Exchange Control Panel (ECP) VDir**, den **Offline Address Book (OAB) VDir Services** sowie weiterer Dienste.

Der Finder der Schwachstelle CVE-2021-26855 [MIC2021g] hat dieser den Namen ProxyLogon gegeben. Auf der entsprechenden Webseite findet sich auch ein Video, mit dem die Ausnutzung gezeigt wird [PRO2021].

Bewertung

Die Schwachstellen sind mit CVSS-Scores von bis zu 9.1 als kritisch zu bewerten – aufgrund der aktiven Ausnutzung und der hohen Wahrscheinlichkeit einer Kompromittierung sollte die Installation der Patches für kurzfristig angestoßen werden.

Zu den angegriffenen Zielen liegen dem BSI keine detaillierten Informationen vor.

Update 1:
Auch wenn Microsoft zunächst ausschließlich Betroffene in den USA benannte, müssen Organisationen mit anfälligen Exchange-Systemen aufgrund der öffentlichen Verfügbarkeit von Proof-of-Concept Exploit-Code, starker weltweiter Scan-Aktivitäten und zahlreichen Berichten über erfolgreiche Angriffe [TWI2021] von einem hohen Angriffsrisiko

ausgehen. Bei verwundbaren Systemen, welche bislang noch nicht gepatcht wurden, sollte von einer Kompromittierung ausgegangen werden.

Update 2:
Das BSI beobachtet eine Vielzahl an Meldungen über kompromittierte Exchange-Server.

Exchange-Server besitzen in vielen Infrastrukturen standardmäßig (teilweise ungerechtfertigt) sehr hohe Rechte im Active Directory. Es ist denkbar, dass weitergehende Angriffe mit den Rechten eines übernommenen Exchange-Servers potenziell mit geringem Aufwand auch die gesamte Domäne kompromittieren können. Zu berücksichtigen ist zudem, dass die Schwachstelle ebenfalls aus dem lokalen Netz ausnutzbar wäre, sofern beispielsweise ein Angreifer über einen infizierten Client auf Outlook Web Access Zugriff erhält.

Auch deshalb sind die entsprechenden Maßnahmen SOFORT und ggf. auch über das Wochenende umzusetzen!

Es gilt zu prüfen, welche begleitenden Maßnahmen diese Eskalation erforderlich macht. (Wirkungsbewertung, Ausweichmaßnahmen, Kunden-/MA-Kommunikation, ...)

Das BSI wertet laufend die verfügbaren Informationen aus und plant kurzfristige Updates der Warnmeldung. Bitte stellen Sie deren unverzügliche Bearbeitung sicher.

Update 3:
Nach Angaben des Herstellers Microsoft hat das Update keine funktionalen Auswirkungen [MIC2021e].

Ein erste Ausnutzung der Schwachstelle im Rahmen gezielter Angriffe konnte laut Volexity in forensischen Analysen bereits im November 2020 festgestellt werden. Daher sollten grundsätzlich alle über das Internet erreichbaren Exchange Server, auch wenn der Patch unmittelbar nach Veröffentlichung eingespielt wurde, auf vorhandene Webshells untersucht werden.

Maßnahmen

Das BSI empfiehlt dringend das Einspielen der von Microsoft bereitgestellten Sicherheitsupdates. Bitte beachten Sie, dass die Updates nur für Server mit aktuellen kumulativen Updates (CU) zur Verfügung stehen. Verwundbar sind allerdings alle CUs. Daher sollten hier die aktuellen Updates eingespielt werden.

Update 1:
Um zu prüfen, ob bereits ein Angriff auf das eigene Netzwerk stattgefunden hat, stellen Microsoft, Volexity und Rapid 7 Indicators of Compromise sowie weitere Anleitungen für die Mitigation zur Verfügung [MIC2021a], [VOL2021], [CIS2021a], [RAP2021].

Anfällige Exchange-Systeme sollten aufgrund des hohen Angriffsrisikos dringend auf entsprechende Auffälligkeiten geprüft werden.

Update 2:
1. Aufgrund einer deutlichen Verschärfung der Bedrohungslage sind die von Microsoft bereitgestellten **Sicherheitsupdates** möglichst **sofortzu installieren**.
2. Sofern eine Aktualisierung nicht sofort möglich ist, muss ein nicht ausschließlich mittels VPN aus dem Internet erreichbarer Outlook Web Access Zugang sofort deaktiviert werden.
   Die Notwendigkeit der Erreichbarkeit von internen Diensten aus dem Internet, wie hier durch Exchange bereitgestellt, sollte unter Berücksichtigung des BSI IT-Grundschutzes (insbesondere NET.1.1 Netzarchitektur und -design - A11, NET.3.3 VPN) kritisch geprüft werden [BSI2021]. Da Exchange-Server immer wieder von kritischen Schwachstellen betroffen sind, die häufig - wie auch in diesem Fall - direkt über einen Fernzugriff aus dem Internet ausgenutzt werden können, besteht hierin eine besondere Wichtigkeit.
3. Bei allen Systemen, die nicht sofort in der Nacht zu Mittwoch aktualisiert wurden, ist **zu prüfen, ob es zu einer Kompromittierung gekommen ist**. Hierzu müssen Exchange-Systeme auf bekannte Webshells untersucht werden.
   1. Von Microsoft wurde ein unter [MIC2021d] abrufbares Detektionsskript veröffentlicht, das die Überprüfung des Exchange-Servers auf eine mögliche Ausnutzung der Schwachstellen ermöglicht.

2. Zur Orientierung bietet [CIS2021b] einen ausführlichen Leitfaden bzgl. des Vorgehens bei der Überprüfung von Exchange-Systemen.

4. Um die Möglichkeit der Angriffsdetektion zu verbessern, sollte die Protokollierung der Exchange-Server und des Active Directory ausgeweitet werden. Hierzu sollte für die lokalen Logs der Speicherplatz erhöht werden und auf dem Domain Controller insbesondere die folgenden Ereignisse überwacht werden:
   1. Logging von Anmeldungen mit dem Computerkonto des Exchange IIS Servers (Event-ID 4624, LogonType=3, Authentication Package=NTLM, Account Name=<Exchange IIS Server>)
   2. Detektion mit Hinblick auf privilegierte Berechtigungen im Active Directory, z. B. durch Logging von Änderungen in hochprivilegierten Gruppen und bei Benutzern (z. B. Veränderung der DACL, Event-ID 5136)
5. Im Falle der Detektion einer Webshell muss das System und entsprechend der Berechtigungen ggf. weitere Systeme wie das Active Directory näher untersucht werden.

Organisationen, die in einem Malware Information Sharing Portal (MISP) Verbund angeschlossen sind, finden im MISP-Event "HAFNIUM - Mass attack on Microsoft Exchange Servers" (UUID: b7636c3e-a515-436b-a646-5ebd750df006) weitere Informationen. Eine statische Momentaufnahme des Events finden Sie auch im Anhang.

Update 3:
Schwachstellen

- Es gilt weiterhin, dass die durch Microsoft bereitgestellten **Sicherheitsupdates** möglichst **sofortzu installieren** sind.
- Unternehmen und Organisationen, welcher außer Stande sind, die jeweilige Microsoft-Exchange-Umgebung unmittelbar zu aktualisieren, sollten die nachfolgenden Maßnahmen umsetzen:
  1. Die Dienste **Unified Messaging (UM)**, **Exchange Control Panel (ECP) VDir**, und **Offline Address Book (OAB) VDir Services müssen deaktiviert** werden. Das Erstellen der Regeln zur Deaktivierung der Dienste ist im Detail in [MIC2021e] beschrieben.
  2. Im Anschluss muss **OWA**, **ActiveSync**, etc. deaktiviert werden.
  3. Dies sollte eine Ausnutzung der Schwachstelle verhindern, bis die notwendigen CU's und das Update aus [MIC2021c] installiert werden können.
  4. Bevor die Dienste wieder mit dem Internet verbunden werden, sollten die Exchange-Server überprüft werden. Hierzu können die Skripte [Exch2021a] und [Mic2021f] benutzt werden.
- Zur Überprüfung der Schwachstelle [MIC2021g] stellt Microsoft eine aktualisierte spezifische NMAP-Regel [MIC2021d] zur Verfügung.
  - › Nach Berichten kann es bei der Nutzung des Skripts mit NMAP in Einzelfällen zu Fehlermeldungen kommen. Zur Behebung sollte beim Aufruf von NMAP der folgende Parameter ergänzt werden: "--min-rtt-timeout 3"

Kompromittierung

- Es ist weiterhin **zu prüfen, ob es zu einer Kompromittierung gekommen ist**. Hierzu müssen Exchange-Systeme auf bekannte Webshells untersucht werden.
- Um eine Überprüfung auf eine Kompromittierung zu ermöglichen, sollte kurzfristig technisch und organisatorisch sichergestellt werden, dass relevante Logs auf dem Server nicht gelöscht oder überschrieben werden. Die Verfahren des jeweils gültigen Notfallprozesses (Datenschutz/Betriebs- oder Personalrat) sind dabei zu berücksichtigen.
- Eine mögliche Shell wurde z. B. unter %PROGRAMFILES%\Microsoft\Exchange Server\V15\FrontEnd\HttpProxy \owa\auth\ als RedirSuiteServerProxy.aspx abgelegt. Generell sind alle kürzlich erzeugten .aspx-Dateien verdächtig. Allerdings könnte eine Webshell auch in bestehende Dateien hinzugefügt werden, indem eine einzige Zeile eingefügt wird. Hinweis: Die RedirSuiteServiceProxy.aspx ist grundsätzlich legitim.
- Falls eine **Webshell** gefunden wird, sollte die Organisation in den **Incident Response Modus** übergehen. Um nachzuvollziehen, welche Befehle über die Webshell abgesetzt wurden, sollte zeitnah ein Arbeitsspeicher-Image erstellt werden. Dazu sollte das ganze System forensisch gesichert werden, um prüfen zu können, ob von diesem System ein Lateral Movement ins eigene Netzwerk erfolgte.
  Es sind die begleitenden Maßnahmen dieser Eskalation zu berücksichtigen. (Wirkungsbewertung, Ausweichmaßnahmen, Kunden-/MA-Kommunikation, ...) Sie finden eine Übersicht zu Incident Response Maßnahmen auf den Webseiten des BSI [BSI2021b].

Grundsätzlich gilt: wenn Sie mit der Bewältigung der Situation (schnelles Patchen, forensische Untersuchungen, etc.) überfordert sind, sollten Sie wegen der möglichen schwerwiegenden Konsequenzen für Ihre Organisation einen IT-Dienstleister hinzuziehen.

Organisationen und Unternehmen, die Unterstützung bei der forensischen Sicherung oder bei der Incident Response benötigen, können sich an einen qualifizierten APT-Response-Dienstleister [BSI2021a] wenden.

Links

[BSI2021] IT-Grundschutz-Kompendium
https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/IT-Grundschutz-Kompendium/it-grundschutz-kompendium_node.html

[BSI2021a] Liste der qualifizierten APT-Response-Dienstleister
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Dienstleister_APT-Response-Liste.html

[BSI2021b] IT-Sicherheitsvorfall, was soll ich tun?
https://www.bsi.bund.de/DE/IT-Sicherheitsvorfall/Kritische-Infrastrukturen-und-meldepflichtige-Unternehmen/Ich-habe-einen-IT-Sicherheitsvorfall-Was-soll-ich-tun/ich-habe-einen-it-sicherheitsvorfall-was-soll-ich-tun.html

[CVE2021d] CISA Alert (AA21-062A) Mitigate Microsoft Exchange Server Vulnerabilities
https://us-cert.cisa.gov/ncas/alerts/aa21-062a

[CIS2021b] CISA Alert (AA21-062A) Mitigate Microsoft Exchange Server Vulnerabilities
https://us-cert.cisa.gov/ncas/alerts/aa21-062a

[Exch2021a] Exchange Server Health Checker script
https://github.com/dpaulson45/HealthChecker#download

[MIC2021a] HAFNIUM targeting Exchange Servers with 0-day exploits
https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

[MIC2021b] Multiple Security Updates Released for Exchange Server
https://msrc-blog.microsoft.com/2021/03/02/multiple-security-updates-released-for-exchange-server/

[MIC2021c] Released: March 2021 Exchange Server Security Updates
https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901

[MIC2021d] Microsoft Security scripts, Detect Hafnium IOCs and Exchange Server SSRF Vulnerability (CVE-2021-26855)
https://github.com/microsoft/CSS-Exchange/tree/main/Security

[MIC2021e] Microsoft Exchange Server Vulnerabilities Mitigations
https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/

[MIC2021f] Microsoft Test-Hafnium script
https://github.com/microsoft/CSS-Exchange/tree/main/Security

[MIC2021g] CVE-2021-26855
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26855

[MIC2021h] CVE-2021-26857
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26857

[MIC2021i] CVE-2021-26858
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26858

[MIC2021j] CVE-2021-27065
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-27065

[PRO2021] ProxyLogon
https://proxylogon.com/

[RAP2021] Rapid7 Response to Microsoft Exchange 0-day
https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day/

[TWI2021] Report about compromise of a honeypot
https://twitter.com/GossiTheDog/status/1367116774504857607

[TWI2021b] Shodan results
https://twitter.com/shodanhq/status/1367525621065261062

[VOL2021] Operation Exchange Marauder: Active Exploitation of Multiple Zero-Day Microsoft Exchange Vulnerabilities
https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

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 TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. 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. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

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:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.