TLP:WHITE

Bundesamt
für Sicherheit in der
Informationstechnik

Microsoft Exchange Schwachstellen

Detektion und Reaktion

CVE-2021-26855, CVE-2021-26857, CVE-2021-26858, CVE-2021-27065

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
Initiale Version v1.0	08.03.2021	Bundesamt für Sicherheit in der Informationstechnik	Ergänzende Informationen zur BSI Warnmeldung
v1.1	09.03.2021	Bundesamt für Sicherheit in der Informationstechnik	Ergänzungen zu Detektionsmöglichkeiten, Korrektur bei URLs
v1.2	09.03.2021	Bundesamt für Sicherheit in der Informationstechnik	Aufnahme weiterer Quellen
v1.3	09.03.2021	Bundesamt für Sicherheit in der Informationstechnik	Aufnahme weiterer Detektionsmöglichkeiten und Quellen
v1.4	09.03.2021	Bundesamt für Sicherheit in der Informationstechnik	Aufnahme weiterer Detektionsmöglichkeiten sowie Hinweis auf ACS-Seite zu APT-Dokumenten

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Internet: https://www.bsi.bund.de

Service-Center (Telefon): 0800 2741000
Service-Center (E-Mail): service-center@bsi.bund.de
Einen Vorfall melden: https://www.allianz-fuer-cybersicherheit.de/Webs/ACS/DE/IT-Sicherheitsvorfall/Unternehmen/Online-Meldung/online-meldung_node.html

Für die Zielgruppen und Partner des BSI gelten darüber hinaus die üblichen Meldewege.

Inhalt

1 Die Intention der Täter 4
2 Wie kann ich erkennen, ob ich betroffen bin? 5
2.1 Auslesen von E-Mails mittels CVE-2021-26855 6
2.2 Auffälligkeiten in den ECP Server Logs 6
2.3 Suche nach Webshells 6
2.4 Web Log User Agents 8
3 Wie kann ich weitere Aktivitäten detektieren? 9
Literaturverzeichnis 11
Abkürzungsverzeichnis 12

1 Die Intention der Täter

Aktuell werden die Exchange-Schwachstellen von mehreren Tätergruppen ausgenutzt, die laut öffentlicher Berichte von Sicherheitsfirmen in der Vergangenheit mit Informationsbeschaffung in Verbindung gebracht wurden. Ziele waren damals Think-Tanks, Universitäten und Nicht-Regierungs-Organisationen sowie Kanzleien und Rüstungsfirmen. Die betroffenen Organisationen waren in der Regel in Nordamerika ansässig und sind bis dahin offenbar sehr gezielt ausgesucht worden (vgl. z.B. [Mic2021a]).

Spätestens seit Bekanntwerden der Schwachstellen hat sich das Verhalten der Täter jedoch stark geändert. Nun werden die Exploits **massenhaft gegen Tausende von Zielen eingesetzt - offenbar weltweit.**

Es ist bisher unklar, ob die geänderte Vorgehensweise auch mit geänderten Intentionen und Zielen einhergeht. Es ist sowohl denkbar, dass das Ziel weiterhin Informationsbeschaffung ist und die Exploits mit maximaler Wirkung eingesetzt werden sollten, bevor Sicherheitsteams weltweit Patches einspielen können. In diesem Fall wird nur ein Bruchteil der kompromittierten Organisationen für die Täter interessant sein - sie benötigen aber zunächst Zeit, um ihre Opfer zu triagieren. Aber auch das Szenario, dass die Täter die Exploits nun finanziell motiviert verwenden und in späteren Schritten relativ großflächig Ransomware oder ähnliches nachladen, ist plausibel (vgl. z.B. auch [CIS2021b]).

Man darf davon ausgehen, dass Sicherheitsfirmen und Medien zeitnah berichten werden, sobald sichtbare Effekte wie Ransomware festgestellt werden. Solange dies nicht der Fall ist, sollte die Hypothese beibehalten werden, dass es sich um Informationsbeschaffungs-Aktivitäten handelt.

2 Wie kann ich erkennen, ob ich betroffen bin?

Die Schwachstellen erlauben es den Tätern, **Mails auszulesen, beliebige Dateien in Serververzeichnisse zu schreiben** und **eigenen Code auf dem Server auszuführen**. Auf diese drei Möglichkeiten sollte geprüft werden. Dafür eigenen sich die im Folgenden beschriebenen Methoden.

ⓘ Hinweis

Die im Folgenden beschriebenen Methoden lassen sich zum Teil automatisiert durch Skripte und geeignete Software überprüfen. Dazu zählen z.B.:

- **Microsoft Test Skript:** https://github.com/microsoft/CSS-Exchange/tree/main/Security
  Das Tool enthält alle IOCs, die in dem Microsoft Blogpost beschrieben werden:
  https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
- **Microsoft Support Emergency Response Tool (MSERT):** Microsoft Defender hat den Microsoft Safety Scanner (MSERT.exe) aktualisiert, um mögliche Ausnutzungen der Microsoft Exchange Schwachstellen zu detektieren. Das Tool kann von Administratoren **für Server** genutzt werden, **die nicht von Microsoft Defender geschützt werden** (Hinweis: Das Tool muss mit dem Argument „/N“ gestartet werden, wenn eventuelle Funde nicht direkt gelöscht werden sollen: msert.exe /N):
  https://msrc-blog.microsoft.com/2021/03/05/microsoft-exchange-server-vulnerabilities-mitigations-march-2021/
- **Microsoft IOC Feed:** Microsoft veröffentlicht bekannte Hashes und maliziöse Dateipfade in einem eigenen Feed. Die Daten sind in JSON und CSV erhältlich:
  https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/MSTICIoCs-ExchangeServerVulnerabilitiesDisclosedMarch2021.csv und
  https://raw.githubusercontent.com/Azure/Azure-Sentinel/master/Sample%20Data/Feeds/MSTICIoCs-ExchangeServerVulnerabilitiesDisclosedMarch2021.json
- **MISP:** 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.
- **Sigma**: Das Sigma Team hat eine Regel veröffentlicht, welche zur Detektion der Exchange Schwachstellen genutzt werden kann:
  https://github.com/SigmaHQ/sigma/blob/master/rules/web/web_exchange_exploitation_hafnium.yml
- **YARA:** Siehe [Rot2021a], [Rot2021b] und [Rup2021]. Als Alternative können auch die Yara Scanner Thor Lite[1] (https://www.nextron-systems.com/thor-lite/) oder Loki (https://github.com/Neo23x0/Loki) genutzt werden
- **CERT.LV Detektions-Skript für Webshells:** Das lettische CERT hat ebenfalls ein eigenes Skript veröffentlicht, mit welchem nach Webshells im Kontext Hafnium gesucht werden kann:
  https://github.com/cert-lv/exchange_webshell_detection
- **Logsuche mit Bordmitteln:** Eric Capuano hat einige Beispielaufrufe bereitgestellt, die zur ersten schnellen Suche in Logs genutzt werden können:
  https://gist.github.com/ecapuano/13386852fb80beac4561f2bed569095e

[1] https://www.nextron-systems.com/2021/03/06/scan-for-hafnium-exploitation-evidence-with-thor-lite/

2.1 Auslesen von E-Mails mittels CVE-2021-26855

Die Ausnutzung der o.a. Schwachstelle kann mittels Log-Einträgen nachvollzogen werden. Im Fall von Outlook on the Web/Outlook Web App (OWA) nutzen die Täter **POST-Anfragen auf statische Inhalte** unter dem Pfad /owa/auth/Current/themes/resources. Mit speziell präparierten SOAP-Payloads ist es den Tätern dann möglich, E-Mails ohne Authentifizierung zu exfiltrieren.

2.2 Auffälligkeiten in den ECP Server Logs

Hinweise für die Ausnutzung der Remote Code Execution Schwachstelle können sich in den **Exchange Control Panel (ECP) Server Logs** finden (in der Regel finden Sie die Logs unter <exchange install path>\Logging\ECP\Server\), da die Ausnutzung im Kontext des Set-OabVirtualDirectory ExchangePowerShell cmdlet stattzufinden scheint [Vol2021].

Es empfiehlt sich daher nach dem **String**
S:CMD=Set-OabVirtualDirectory.ExternalUrl='"
zu suchen (*Hinweis: Der String könnte so oder so ähnlich aussehen*).

2.3 Suche nach Webshells

Ein typisches Vorgehen der Täter ist es, mit Ausnutzung der RCE-Schwachstelle eine Webshell auf dem Server zu hinterlassen, um weitere Befehle auszuführen.

> ☝ **Wichtiger Hinweis**
>
> Durch die sehr breite Ausnutzung der Schwachstelle ist davon auszugehen, dass nicht nur die Webshells zum Einsatz kommen, über die kürzlich im Kontext der Gruppe Hafnium durch Microsoft und Volexity berichtet wurde.

Mindestens die folgenden Webshells wurden bereits im Zusammenhang mit der Ausnutzung der Exchange-Schwachstelle beobachtet:

- SIMPLESEESHARP
- SPORTSBALL
- China Chopper
- ASPXSPY
- reGeorg

Daher ist es sinnvoll, sowohl spezifisch als auch generisch nach Webshells zu suchen:

- Die YARA-Regeln unter [Rot2021b] helfen bei der Suche nach Webshells im Kontext Hafnium.
- Die YARA-Regeln unter [Rup2021] helfen bei der Suche nach generischen Webshells.

Im Zusammenhang mit den Exchange Schwachstellen sind zudem ASPX-Dateien in den folgenden Verzeichnissen und Unterverzeichnissen [Vol2021] auffällig[2]:

- \inetpub\wwwroot\aspnet_client\
- \<exchange install path>\FrontEnd\HttpProxy\ecp\auth\
  (lediglich TimeoutLogoff.aspx ist legitim)
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\Current\
- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\<Versionsnummer>\

Etwas aufwändiger ist die Suche in folgendem Verzeichnis, das bei einer Standard-Installation ASPX-Dateien enthält. Webshells können auch in diese legitimen Dateien eingefügt werden, indem eine einzige Zeile ergänzt wird.

- \<exchange install path>\FrontEnd\HttpProxy\owa\auth\
  (Dateien, die nicht mehr dem Stand der Standard-Installation entsprechen)

Bei Internet Information Service (IIS)-Webservern werden ASP-Dateien zu temporären Bibliotheken kompiliert. Die Dateien mit dem Namen app_web__[a-zA-Z0-9]{8}.dll können auch eine mögliche Webshell enthalten (siehe nachfolgende YARA-Regel).

```
rule apt_Hafnium_Compiled_Webshell {
   meta:
      description = "Triggers on suspicious compiled ASP DLL files with JScriptEvaluate call. Results does not have to be related to Hafnium cluster."
      author = "Bundesamt für Sicherheit in der Informationstechnik"
      date = "2021-03-05"
   strings:
      $regex1 = /\~\/aspnet_client\/system_web\/[a-zA-Z0-9]{8}\.aspx/ ascii wide fullword
      $regex2 = /App_Web_[a-zA-Z0-9]{8}.dll/ ascii wide fullword
      $regex3 = /aspnet_client_system_web_[a-zA-Z0-9]{8}_aspx/ ascii wide fullword
      $s1 = "OAB" ascii wide
      $s2 = "JScriptEvaluate" ascii wide
   condition:
      uint16(0) == 0x5a4d and filesize < 40KB and all of them
}
```

[2] Die NCC Group hat ein GitHub Respository veröffentlicht, in dem sie die Hashwerte der Dateien in den Exchange-Installationsverzeichnissen aus den Installationspaketen zur Verfügung stellen, was ggf. als Abgleich für die Suche nach Webshells hilfreich sein kann: https://github.com/nccgroup/Cyber-Defence/tree/master/Intelligence/Exchange
(vgl. auch https://twitter.com/NCCGroupInfosec/status/1368466300515844096).

2.4 Web Log User Agents

Volexity erwähnt auch einige User-Agents, die zwar nicht als eindeutige Indikatoren für eine Kompromittierung zu verstehen sind, jedoch als weitere Anhaltspunkte dienen können, wenn ein Kompromittierungsverdacht besteht [Vol2021].

POST Requests zu den Dateien in den Ordnern unter /owa/auth/Current

DuckDuckBot/1.0;+(+http://duckduckgo.com/duckduckbot.html)
facebookexternalhit/1.1+(+http://www.facebook.com/externalhit_uatext.php)
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)
Mozilla/5.0+(compatible;+Bingbot/2.0;++http://www.bing.com/bingbot.htm)
Mozilla/5.0+(compatible;+Googlebot/2.1;++http://www.google.com/bot.html
Mozilla/5.0+(compatible;+Konqueror/3.5;+Linux)+KHTML/3.5.5+(like+Gecko)+(Exabot-Thumbnails)
Mozilla/5.0+(compatible;+Yahoo!+Slurp;+http://help.yahoo.com/help/us/ysearch/slurp)
Mozilla/5.0+(compatible;+YandexBot/3.0;++http://yandex.com/bots)
Mozilla/5.0+(X11;+Linux+x86_64)+AppleWebKit/537.36+(KHTML,+like+Gecko)+Chrome/51.0.2704.103+Safari/537.36

Auffällige User-Agents im Kontext der Ausnutzung der /ecp/ URLs

ExchangeServicesClient/0.0.0.0
python-requests/2.19.1
python-requests/2.25.1

Auffällige User-Agents im Kontext des Post-Exploitation-Zugriffs auf Webshells

antSword/v2.1
Googlebot/2.1+(+http://www.googlebot.com/bot.html)
Mozilla/5.0+(compatible;+Baiduspider/2.0;++http://www.baidu.com/search/spider.html)

3 Wie kann ich weitere Aktivitäten detektieren?

Wichtiger Hinweis

Eine weitergehende Kompromittierung der Domäne ist durch die im Standard vorhandenen hohen Rechte der Exchange Server im Active Directory verhältnismäßig einfach möglich. **Es sollte auf eine weitergehende Kompromittierung des ADs bspw. mit den Rechten des Exchange Servers oder durch Hinzufügen von neuen Benutzern mit hochprivilegierten Rechten geprüft werden.**
Es ist möglich, dass die Active Directory Datenbank (ntds.dit) bspw. über ein nach außen verfügbares Exchange-Verzeichnis ausgeleitet wurde.

Dumpen von Credentials aus dem Speicher

Die Angreifer verwenden u.a. Procdump, um den LSASS Prozessspeicher zu dumpen:

```
C:\windows\temp\procdump64 -accepteula -ma lsass.exe C:\windows\temp\lsass
```

Das Dumpen des LSASS Prozessspeichers via Procdump hinterlässt ein Artefakt in Form eines „EulaAccepted"-Eintrags mit dem Wert „1" in der Registry unter HKEY_USERS\<SID des verwendeten Benutzers>\Software\Sysinternals\ProcDump, welches auf dem betroffenen Server geprüft werden kann.

Laut [Vol2021] wurde der LSASS Prozessspeicher in manchen Fällen auch mit Hilfe von comsvcs.dll gedumpt, da comsvcs.dll als LOLBin nativ auf den Servern vorhanden ist:

```
rundll32 C:\windows\system32\comsvcs.dll / MiniDump lsass.dmp
```

Alternativ verwenden die Täter auch eine spezielle Variante von Mimikatz. Diese wurde mit dem Dateinamen CreateRemoteThreadTest.exe und dem SHA-256-Hash 173ac2a1f99fe616f5efa3a7cf72013ab42a68f7305e24ed795a98cb08046ee1 verwendet [Rap2021].

Staging

In einigen Fällen haben die Täter Daten, die sie stehlen wollen, per 7Zip in ZIP-Archiven zusammengefasst [Mic2021b]. Die Existenz unerwarteter ZIP-Dateien (mit meist kurzen Namen und in Verzeichnissen wie "ProgramData\" kann daher ein Hinweis auf Exfiltration sein.

Nachladen von Tools

Vereinzelt haben die Täter PowerCat von Github heruntergeladen und verwendet. Es kann daher geprüft werden, ob die URL https://raw.githubusercontent.com/besimorhino/powercat/master/powercat.ps1 in den Log-Daten auftaucht. Falls PowerCat nicht von den Administratoren selbst verwendet wird, kann geprüft werden, ob die Datei powercat.ps1 auf dem System vorhanden ist.

Umbenennen von cmd.exe

Bei Bedarf haben die Täter die cmd.exe in "ProgramData\" kopiert und ggf. umbenannt.

DLL-Side-Loading

Um weitere Backdoors zu installieren, verwenden die Täter DLL-Side-Loading. Zu diesem Zweck wird eine legitime Anwendung (wie z.B. AppLaunch.exe) in einen kurzen Dateinamen umbenannt und zusammen mit einer maliziösen DLL in ein Verzeichnis wie "ProgramData\" kopiert. Die Existenz einer unerwarteten Datei mit zweistelligem Dateinamen und .exe-Dateiendung zusammen mit einer DLL kann also ein Hinweis auf Aktivität der Täter sein.

Weitere spezifische Hinweise

Weitere sehr detaillierte Hinweise (auf Englisch) finden sich auch unter [Blu2021], [Ham2021], [Fir2021] und [CIS2021a], [CIS2021b].

Weitere generische Hinweise

Viele weitere Hinweise zur Detektion von Advanced Persistent Threats sowie zur Reaktion bei Hinweisen auf eine Kompromittierung finden Sie auch in den nachfolgend aufgeführten BSI-Publikationen:

TLP:AMBER Advanced Persistent Threats – Teil 3 Detektion
Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung
Anlassbezogene und akute Hilfestellungen, BSI 2021

TLP:WHITE, in Teilen TLP:AMBER Advanced Persistent Threats – Teil 4 Reaktion
Technische und organisatorische Maßnahmen für die Vorfallsbearbeitung
Anlassbezogene und akute Hilfestellungen, BSI 2021

TLP:GREEN Advanced Persistent Threats – Teil 5 Reaktion
Strategische Maßnahmen zur Reaktion für das Management
Wo zieht man im Angriffsfall rote Linien?, BSI 2021

ⓘ Hinweis

Weitere Informationen zu den genannten APT-Dokumenten finden Sie unter:

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Empfehlungen-nach-Gefaehrdungen/APT/apt.html

Bitte beachten Sie, dass die Dokumente aufgrund der Einstufung z.T. nur über den internen Bereich der ACS bzw. nur im internen INSI-Bereich der ACS verfügbar sind.

Literaturverzeichnis

Blu2021 Blue Team Blog, Microsoft Exchange Zero Day's – Mitigations and Detections, https://blueteamblog.com/microsoft-exchange-zero-days-mitigations-and-detections

CIS2021a Cybersecurity & Infrastructure Security Agency (CISA), Alert (AA21-062A) Mitigate Microsoft Exchange Server Vulnerabilities, https://us-cert.cisa.gov/ncas/alerts/aa21-062a

CIS2021b Cybersecurity & Infrastructure Security Agency (CISA), Remediating Microsoft Exchange Vulnerabilities, https://us-cert.cisa.gov/remediating-microsoft-exchange-vulnerabilities

Fir2021 FireEye, Threat Research: Detection and Response to Exploitation of Microsoft Exchange Zero-Day Vulnerabilities, https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-vulnerabilities.html

Ham2021 John Hammond, Rapid Response: Mass Exploitation of On-Prem Exchange Servers, https://www.huntress.com/blog/rapid-response-mass-exploitation-of-on-prem-exchange-servers

Mic2021a Microsoft, New nation-state cyberattacks, https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/

Mic2021b Microsoft, HAFNIUM targeting Exchange Servers with 0-day exploits, https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/

Rap2021 Rapid7, https://blog.rapid7.com/2021/03/03/rapid7s-insightidr-enables-detection-and-response-to-microsoft-exchange-0-day/

Rot2021a Florian Roth, apt_hafnium_log_sigs.yar, https://github.com/Neo23x0/signature-base/blob/master/yara/apt_hafnium_log_sigs.yar

Rot2021b Florian Roth, apt_hafnium.yar, https://github.com/Neo23x0/signature-base/blob/master/yara/apt_hafnium.yar

Rup2021 Arnim Rupp, gen_webshells.yar, https://github.com/Neo23x0/signature-base/blob/master/yara/gen_webshells.yar

Vol2021 Volexity, 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/

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
DLL	Dynamic Link Library
ECP	Exchange Control Panel
IIS	Internet Information Service
IOC	Indicators of Compromise
MISP	Malware Information Sharing Platform
OWA	Outlook Web App
RCE	Remote Code Execution