ADVANCED
ANALYTICS

G DATA **ADVANCED ANALYTICS**

Ad-hoc Handlungsempfehlungen zu den MS Exchange-Schwachstellen CVE-2021-26855 et al. (HAFNIUM)

Guideline v.1.5. 16. März 2021

G DATA Advanced Analytics GmbH
G DATA Campus · Königsallee 178
D-44799 Bochum, Germany
T: +49 234 9762-820
M: info@gdata-adan.de

Zusammenfassung

Seit Anfang Januar sind Microsoft Schwachstellen in mehreren Versionen des Exchange-Servers bekannt (CVE-2021-26885 et al.). Die Schwachstellen wurden initial von einem staatlichen Akteur ausgenutzt, den Microsoft *HAFNIUM* nennt. Inzwischen ist davon auszugehen, dass weitere Akteure im Besitz von funktionierendem Code sind, der geeignet ist, die Schwachstelle auszunutzen und eine Kompromittierung herbeizuführen. Stand 08.03.2021 geht das BSI von mindestens 26000 verwundbaren Exchange-Instanzen in Deutschland aus[1].

Uns erreicht eine Vielzahl von Anfragen von betroffenen oder möglicherweise betroffenen Unternehmen. Dieses Dokument enthält Handlungsempfehlungen zur ad-hoc Schadensbegrenzung für möglicherweise betroffene Unternehmen.

[1] `https://twitter.com/certbund/status/1369009516893855759`

Ad-hoc Maßnahmen

Wenn nicht ausgeschlossen werden kann, dass eine Kompromittierung von einem oder mehreren Computersystemen vorliegt, empfehlen wir mindestens folgende Maßnahmen durchzuführen:

1. Zugriff auf das Webinterface des Exchange-Servers oder -clusters übergangsweise unterbinden (typischerweise https, TCP Port 443), mindestens bis zur Behebung der Schwachstelle, optimalerweise bis zur Verifikation, dass kein unerwünschter Zugriff auf oder über das System stattgefunden hat.
2. Funktionsfähige *Offline*backups sicherstellen.
3. Exchange-Server patchen[2]

Handlungsempfehlungen zur Verminderung von Informationsverlust

Folgende Maßnahmen können eine eventuell notwendige forensische Aufarbeitung erleichtern oder überhaupt ermöglichen:

1. Vor jeglichen Handlungen sollte ein Snapshot inkl. Arbeitsspeicher von virtuellen Systemen erstellt werden, um eventuell vorhandene forensische Spuren zu erhalten
2. Vorhandene Logs offline sichern
3. Logeinstellungen anpassen und Logs täglich offline sichern

Empfohlene minimale Logvolumina bei täglicher Sicherung:

	Arbeitsplatz	**Server**	**Domaincontroller**
Anwendung/Application	20 MB	100 MB	100 MB
System	20 MB	500 MB	500 MB
Sicherheit/Security	500 MB	2 GB	>2 GB
Windows Powershell	500 MB	1 GB	1 GB
PowerShell Operational	500 MB	1 GB	1 GB

[2] `https://techcommunity.microsoft.com/t5/exchange-team-blog/released-march-2021-exchange-server-security-updates/ba-p/2175901`

Erkennen von möglicherweise betroffenen Systemen

Führen Sie folgende Schritte durch:

1. Stellen Sie sicher, dass all Ihre Exchange-Server gepatcht sind. Wenn Sie nicht sicher sind, ob Ihnen alle eventuell anfälligen Systeme in Ihrer Organisation bekannt sind, kann ein von Microsoft bereitgestelltes `nmap`-Script Sie dabei unterstützen, diese verbliebenen Systeme zu erkennen. Das Script kann hier heruntergeladen werden: `https://raw.githubusercontent.com/microsoft/CSS-Exchange/main/Security/http-vuln-cve2021-26855.nse`

2. Sichern Sie alle `.aspx`-Dateien aus den nachfolgenden Verzeichnissen, insbesondere wenn diese neu angelegt wurden und/oder Ihnen nicht auf Anhieb bekannt erscheinen:
   - `%PROGRAMFILES%\Microsoft\Exchange Server\V15\frontend\httpproxy\owa\auth`
   - `%PROGRAMFILES%\Microsoft\Exchange Server\V15\frontend\httpproxy\ecp\auth`
   - `C:\inetpub\wwwroot`

3. Microsoft hat ein Powershell-Script bereitgestellt, das die Prüfung auf Hinweise für eine Kompromittierung (Indicators of Compromise, IOCs) automatisiert. Die Ausgabe des Scripts kann zur Ersteinschätzung bzgl. einer möglichen Kompromittierung dienen und sollte archiviert werden. Das Script kann hier heruntergeladen werden: `https://github.com/microsoft/CSS-Exchange/releases/latest/download/Test-ProxyLogon.ps1`

4. Das Microsoft Support Emergency Response Tool (MSERT) kann bei der Erkennung einer erfolgreichen Kompromittierung unterstützen: Es erlaubt einen automatischen IOC-Scan der .aspx-Dateien auf typische Webshell-Inhalte und wird seitens Microsoft unter nachfolgendem URL bereitgestellt: `https://github.com/microsoft/CSS-Exchange/blob/main/Security/Defender-MSERT-Guidance.md` Die Durchführung eines *Full Scans* ist empfohlen.

5. Gleichen Sie die Dateipfade der `.aspx`-Dateien, die Sie in Schritt 2 gesichert haben, mit der Ausgabe des MSERT ab, ob diese Webshell-Inhalte aufweisen.

6. Archivieren Sie die Ausgabe des o. g. Powershell-Scripts, des MSERT sowie alle `.aspx`-Dateien, die Sie in Schritt 2 gesichert haben und legen Sie diese in einem gemeinsamen Ordner ab. Komprimieren Sie diesen Ordner als verschlüsselte .zip Datei mit dem Passwort `infected`.

Quellenhinweise

1. https://www.microsoft.com/security/blog/2021/03/02/hafnium-targeting-exchange-servers/
2. https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-197772-1132.pdf?__blob=publicationFile&v=11