SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zehntausende deutscher Microsoft Exchange Server haben kritische Sicherheitslücken

CSW-Nr. 2020-252437-1131, Version 1.1, 13.10.2020

IT-Bedrohungslage*: 3 / Orange

Sachverhalt

Seit mehreren Monaten stehen von Microsoft für die unter CVE-2020-0688, CVE-2020-0692 und CVE-2020-16875 geführten Sicherheitslücken des Groupware- und E-Mail-Servers Exchange Sicherheitsupdates bereit [MS2020a, MS2020b, MS2020c].

Bei CVE-2020-0688 handelt es sich um eine Static Key Schwachstelle im Microsoft Exchange Control Panel (ECP) die unter Verwendung eines gestohlenen E-Mail-Kontos die volle Systemkompromittierung ermöglicht. CVE-2020-0692 erlaubt die Eskalation von Privilegien.

Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

- Microsoft Exchange Server 2010 SP 3 Update RU30 (CVE-2020-0688)
- Microsoft Exchange Server 2013 Cummulative Update 23
- Microsoft Exchange Server 2016 Cummulative Update 14 und 15
- Microsoft Exchange Server 2019 Cummulative Update 3 und 4

Ebenso betroffen sind ältere Produktversionen.

Bei CVE-2020-16875 handelt es sich um eine durch die fehlerhafte Argument-Validierung des New-DlpPolicy cmdlet bedingte Sicherheitslücke, die nach vorheriger Authentisierung ebenfalls Remote Code Execution erlaubt.

Update 1:
Betroffen sind die folgenden Produktversionen, sofern der Einzelpatch zur Behebung der Schwachstelle nicht installiert wurde:

* 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.

- Microsoft Exchange Server 2016 Cummulative Update 16 und 17
- Microsoft Exchange Server 2019 Cummulative Update 5 und 6

Ebenso betroffen sind ältere Produktversionen.

Für beide Sicherheitslücken wurde PoC-/Exploit-Code veröffentlicht [Rap2020a, Soi2020]. Zumindest die Ausnutzung der Sicherheitslücke CVE-2020-0688 wurde bereits im Rahmen gezielter Angriffe beobachtet [Ten2020, Vol2020].

Bewertung

Die anfälligen Dienste der Microsoft Exchange Server sollten grundsätzlich nicht öffentlich erreichbar sein [BSI2020]. Trotzdem sind nach wie vor viele Exchange-Server über EWS öffentlich erreichbar und mehrere Tausend Exchange-Server anfällig für CVE-2020-0688 [Rap2020a]. Die von der Firma Rapid 7 veröffentlichten Zahlen konnten seitens BSI für Deutschland validiert werden und weisen auf ein **Grundproblem bei der sicheren Konfiguration und dem Einspielen kritischer Sicherheitsupdates** hin [Rap2020b].

Eine besondere Kritikalität besteht, da die **Sicherheitslücken entfernt direkt aus dem Internet ausnutzbar** sind und der zugehörige **Angriffscode veröffentlicht bzw. bereits in bekannte Angriffswerkzeuge integriert** wurde. Exchange-Server werden zudem häufig eng in das Active Directory integriert. Da Computer-Konten und Service-Accounts entgegen der Herstellerempfehlung mit priveligierten Rechten - vergleichbar mit Domänen-Administratoren , versehen werden, kann ein Angreifer über die Kompromittierung eines Exchange-Servers somit je nach Systemumgebung schnell in den Besitz von Domänen-Administrator-Credentials gelangen.

Maßnahmen

Das BSI empfiehlt zu prüfen, ob verwundbare Versionen eingesetzt werden und diese schnellstmöglich zu aktualisieren. Weiterhin ist zu prüfen, über welche Protokolle der Exchange-Server über das Internet erreichbar sein muss. Um das Risiko zu minimieren, sollte die Erreichbarkeit auf unbedingt notwendige Protokolle und berechtigte Personen reduziert werden. Dies könnte durch den Einsatz eines VPN-Gateways erreicht werden.

Update 1:
Auch MÜSSEN Dienste, die z.B. aus einer DMZ heraus über das Internet erreichbar sind, von internen Diensten sicher entkoppelt sein. Für die Erbringung solcher Dienste MÜSSEN die benötigten Informationen, die durch interne Dienste verwaltet werden, in einem PUSH-Verfahren vom internen, vertrauenswürdigen Netz in den weniger vertrauenswürdigen DMZ-Bereich repliziert werden. Eine Kompromittierung des Dienstes in der DMZ DARF dabei keinen Einfluss auf die Sicherheit des internen Dienstes haben [BSI2020].

Das CERT-Bund des BSI benachrichtigt ab heute deutsche Netzbetreiber zu bekannten IP-Adressen verwundbarer und über das Internet erreichbarer Exchange-Server in ihren Netzen.

Weiterhin weist das BSI darauf hin, dass Exchange 2010 am 13. Oktober 2020 den End of Support (EoS) Status erreicht. Ab diesem Zeitpunkt werden keinerlei Sicherheitsupdates mehr zur Verfügung gestellt. Auch das EoS-Datum für Exchange 2013 steht bereits fest (11. April 2023). Um sicher zu stellen, dass zukünftig Updates für kritische Sicherheitslücken angewendet werden können, sollten Exchange 2013 nutzende Organisationen zeitnah mit der Migrationsplanung beginnen.

Links

BSI2020 - IT-Grundschutz NET.1.1.A11
https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/NET/NET_1_1_Netzarchitektur_und_-design.html

MS2020a - CVE-2020-0688 | Microsoft Exchange Validation Key Remote Code Execution Vulnerability
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688

MS2020b - CVE-2020-0692 | Microsoft Exchange Server Elevation of Privilege Vulnerability
https://portal.msrc.microsoft.com/de-de/security-guidance/advisory/CVE-2020-0692

MS2020c - CVE-2020-16875 | Microsoft Exchange Server Remote Code Execution Vulnerability
https://portal.msrc.microsoft.com/de-de/security-guidance/advisory/CVE-2020-16875

MS2020d - Description of the secuity update for Microsoft Exchange Server 2019 and 2016
https://support.microsoft.com/en-us/help/4536987/security-update-for-exchange-server-2019-and-2016

Rap2020a - Phishing for SYSTEM on Microsoft Exchange (CVE-2020-0688)
https://blog.rapid7.com/2020/04/06/phishing-for-system-on-microsoft-exchange-cve-2020-0688/

Rap2020b - Microsoft Exchange 2010 End of Support & Patching Study
https://blog.rapid7.com/2020/09/29/microsoft-exchange-2010-end-of-support-and-overall-patching-study/

Soi2020 - SRC-2020-0019 : Microsoft Exchange Server DlpUtils AddTenantDlpPolicy Remote Code Execution Vulnerability
https://srcincite.io/advisories/src-2020-0019/

Ten2020 - CVE-2020-0688: Microsoft Exchange Server Static Key Flaw Could Lead to Remote Code Execution
https://www.tenable.com/blog/cve-2020-0688-microsoft-exchange-server-static-key-flaw-could-lead-to-remote-code-execution

Vol2020 - Microsoft Exchange Control Panel (ECP) Vulnerability CVE-2020-0688 Exploited
https://www.volexity.com/blog/2020/03/06/microsoft-exchange-control-panel-ecp-vulnerability-cve-2020-0688-exploited/