Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Neue Schwachstellen in Microsoft Exchange Server

CSW-Nr. 2021-207541-1032, Version 1.0, 13.04.2021

IT-Bedrohungslage*: 2 / Gelb

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

Am Dienstag, den 13. April 2021, um 19 Uhr MESZ hat Microsoft im Rahmen seines Patchdays auch Updates für Exchange Server veröffentlicht [MIC2021a]. Diese schließen 4 Schwachstellen die Tätern die Möglichkeit bieten, aus der Ferne Code auf dem Server auszuführen.

Bei den Schwachstellen handelt es sich um:

- CVE-2021-28480 Microsoft Server Remote Code Execution Vulnerability [MIC2021b]
- CVE-2021-28481 Microsoft Server Remote Code Execution Vulnerability [MIC2021c]
- CVE-2021-28482 Microsoft Server Remote Code Execution Vulnerability [MIC2021d]
- CVE-2021-28483 Microsoft Server Remote Code Execution Vulnerability [MIC2021e]

Nach Angaben des Herstellers sind die Schwachstellen kritisch.

Sicherheitsupdates stehen für die folgenden Versionen zur Verfügung:

- Exchange Server 2013 CU23
- Exchange Server 2016 CU19 und CU20
- Exchange Server 2019 CU8 und CU9

* 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.

Bewertung

Die Schwachstellen sind mit CVSS-Scores von bis zu 9,8 als kritisch zu bewerten.

Sie wurden im Rahmen eines Coordinated Vulnerability Disclosure an Microsoft gemeldet und sind noch nicht öffentlich.

Da Exchange Server aber gerade im besonderen Fokus der Angreifer stehen, ist mit einer hohen Wahrscheinlichkeit mit einer baldigen Ausnutzung zu rechnen. Die Installation der Patches sollte daher kurzfristig durchgeführt werden. Ein Zusammenhang zu den Exchange Schwachstellen von Anfang März (BSI CSW-Nr. 2021-197772) scheint nicht zu bestehen.

Maßnahmen

Das BSI empfiehlt dringend das Einspielen der von Microsoft bereitgestellten Sicherheitsupdates [MIC2021a].
Bitte beachten Sie, dass die Updates nur für Server mit aktuellen kumulativen Updates (CU) zur Verfügung stehen. Verwundbar sind allerdings alle CUs.

Grundsätzlich sollten auch alle sonstigen Sicherheitsupdates [MIC2021f], die Microsoft im Rahmen des Patchdays veröffentlicht zeitnah installiert werden.

Links

[MIC2021a] April 2021 Update Tuesday packages now available
https://msrc-blog.microsoft.com/2021/04/13/april-2021-update-tuesday-packages-now-available/

[MIC2021b] CVE-2021-28480 Microsoft Server Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28480

[MIC2021c] CVE-2021-28481 Microsoft Server Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28481

[MIC2021d] CVE-2021-28482 Microsoft Server Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28482

[MIC2021e] CVE-2021-28483 Microsoft Server Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-28483

[MIC2021f] Microsoft Security Update Guide
https://msrc.microsoft.com/update-guide

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.