Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Neuer 0-Day Exploit in Microsoft Exchange Server

CSW-Nr. 2022-258168-1332, Version 1.3, 21.12.2022

IT-Bedrohungslage*: 3 / Orange

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 28. September veröffentlichte das Cyber-Sicherheitsunternehmen GTSC einen Blogbeitrag zu neuen Zero-Day Exploits in Microsoft Exchange Servern [GTSC2022]. Demnach wurden im Rahmen einer Analyse eines Vorfalls Hinweise auf eine aktive Ausnutzung von zwei Sicherheitslücken entdeckt. Diese waren in der Lage, auch vollständig gepatchte Systeme zu kompromittieren.

Microsoft hat hierzu einen Beitrag auf seiner Webseite veröffentlicht [MSRC2022]. Darin wird angegeben, dass die Schwachstellen eine Server-Side Request Forgery (CVE-2022-41040) sowie eine Remote Code Execution (CVE-2022-41082) ermöglichen, wenn der Angreifer Zugriff auf PowerShell hat. Hierfür sei allerdings ein authentifizierter Zugriff auf den verwundbaren Server nötig.

Verwundbar seien laut Microsoft die Microsoft Exchange Server 2013, 2016, und 2019.

Gemäß Common Vulnerability Scoring System (CVSS) wurden die Schwachstellen hinsichtlich ihres Schweregrads mit 8.8 bzw. 6.3 von 10 Punkten als "hoch" bzw. "mittel" eingestuft.

Update 1:
In Anlehnung an die im vergangenen Jahr entdeckten Sicherheitslücken in Microsoft Exchange werden die nun bekannt gewordenen Schwachstellen in den Sozialen Medien unter dem Namen "ProxyNotShell" diskutiert [TWIT2022a].

* 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.

Update 3:
Am 20. Dezember 2022 veröffentlichte das IT-Sicherheitsunternehmen CrowdStrike neue Erkenntnisse darüber, dass die hier beschriebenen Schwachstellen derzeit in zusätzlicher Form ausgenutzt werden [CROW2022]. Demnach wäre es den Angreifenden möglich, die von Microsoft veröffentlichten Mitigationsmaßnahmen zu umgehen und Schadsoftware auf den Zielsystemen zu installieren. Dabei wird Outlook Web Access (OWA) als Einfallstor verwendet, um in der "OWASSRF" genannten Attacke die Schwachstellen CVE-2022-41080 [MSRC2022b] und CVE-2022-41082 [MSRC2022c] zu nutzen. Hierüber ist es den Tätern möglich, aus der Ferne Code auszuführen. Tools zur Durchführung des Angriffs kursieren bereits im Internet.

Bewertung

Komponenten der E-Mailinfrastruktur stellen grundsätzlich attraktive Ziele für Angreifer dar. In diesem Zusammenhang stehen auch Microsoft Exchange Server immer wieder im besonderen Fokus der Täter.

Da die Schwachstellen bereits aktiv von Angreifern ausgenutzt werden, besteht auch für deutsche Institutionen die erhöhte Gefahr einer Kompromittierung.

Update 3:
Durch die Veröffentlichung von Tools zur Durchführung von Angriffen welche die unzureichend behobene Schwachstelle ausnutzen, besteht erhöhte Gefahr einer Kompromittierung.

Maßnahmen

Nutzer von Microsoft Exchange Online sind nach Aussage von Microsoft nicht betroffen.

Kunden mit On-Premise Lösungen sollten die im Microsoft-Blog aufgeführten Mitigationsmaßnahmen umsetzen, da zum jetzigen Zeitpunkt noch kein Sicherheitsupdate bekannt ist, welches die Schwachstellen behebt. Dabei wird eine Regel unter dem "IIS Manager -> Default Web Site -> Autodiscover -> URL Rewrite -> Actions" erstellt, welche die bekannten Exploits blockiert:

- IIS Manager öffnen
- "Default Web Site" erweitern
- "Autodiscover" auswählen
- In der Feature-Übersicht auf "URL Rewrite" klicken
- In der Aktions-Spalte auf der rechten Seite eine neue Regel hinzufügen
- "Request Blocking" auswählen und OK drücken
- Die Zeichenkette ".*autodiscover\.json.~~*\@~~.*Powershell.*" (ohne Anführungszeichen) einfügen und OK drücken
- **Unter "Using" die Option "Regular Expression" auswählen**
- Die neue Regel unter "Bedingungen" editieren
- Die Bedingung von {URL} zu ~~{REQUEST_URI}~~**{UrlDecode:{REQUEST_URI}}** ändern

Diese Anleitung befindet sich bebildert unter [MSRC2022]. Nach Aussagen von Microsoft sind keine Funktionseinschränkungen beim Betrieb von Exchange Server zu erwarten. Hinweise zur Erkennung einer bereits erfolgten Kompromittierung werden ebenfalls aufgeführt.

Unabhängig von den konkreten Schutzmaßnahmen in diesem Sachverhalt sollten IT-Sicherheitsverantwortliche stets dafür sorgen, dass die Patchstände der betriebenen Systeme aktuell sind [BSI2022]. Untermauert wird diese Notwendigkeit auch damit, dass Microsoft Out Of Band Patches in der Vergangenheit bei ähnlichen Situationen zunächst priorisiert für das aktuellste CU (Cumulative Update) von Exchange zur Verfügung gestellt hat.

Update 1:
Inzwischen kommen verschiedene IT-Sicherheitsforscher zu der Erkenntnis, dass die von Microsoft herausgegebene Regel zur Blockierung des Exploits nicht immer zielführend ist. Stattdessen wird eine Modifikation der Zeichenkette auf: ".*autodiscover\.json.*Powershell.*" vorgeschlagen [TWIT2022b]. Eine offizielle Stellungnahme des Herstellers steht jedoch noch aus.

Währenddessen hat Microsoft seinen Blogbeitrag zur Mitigation und Detektion von Angriffen aktualisiert [MSRC2022]. Zu den Anpassungen zählt unter anderem, dass bei der Erstellung der Filterregel unter "Using" die Option "Regular Expression" ausgewählt werden sollte. Weiterhin bietet der Hersteller nun ein Skript zur Mitigation mittels URL-Rewrite an. Bei Systemen mit aktiviertem Exchange Emergency Mitigation Service (EEMS) wurde diese Mitigation für Exchange Server 2016 und Exchange Server 2019 bereits automatisch aktiviert.

Außerdem empfiehlt Microsoft, den Zugriff auf PowerShell für Nicht-Administratoren zu deaktivieren. Umsetzungshinweise hierzu hat Microsoft unter [MSRC2022a] veröffentlicht.

IT-Sicherheitsverantwortliche sollten die Umsetzung der ergänzten/modifizierten Maßnahmen schnellstmöglich prüfen.

Update 2:
In weiteren Aktualisierungen des Blogbeitrags wurde u.a. die unter Update 1 vorgeschlagene Modifikation der Blockierungsregel durch Microsoft bestätigt [MSRC2022]. Zusätzlich sollte die zunächst veröffentlichte Bedingung von {REQUEST_URI} zu {UrlDecode:{REQUEST_URI}} korrigiert werden. Die Ausführungen weiter oben wurden entsprechend angepasst. Weiterhin empfiehlt Microsoft, die bereits eingerichtete Regel zu löschen und neu aufzusetzen, anstatt die vorherige Regel zu editieren.

Diese Änderungen hat der Hersteller auch in seinen Unterstützungsangeboten Exchange Emergency Mitigation Service (EEMS) und Exchange On-premises Mitigation Tool v2 (EOMTv2) vorgenommen. Falls das Mitigationsskript manuell bezogen und ausgeführt wurde, müssen Download und Ausführung erneut angestoßen werden, um die Änderungen anzuwenden.

IT-Sicherheitsverantwortliche sollten [MSRC2022] regelmäßig prüfen, da auch weitere Updates in den kommenden Tagen nicht ausgeschlossen werden können.

Update 3:
Auf Basis der neuen Berichte muss davon ausgegangen werden, dass die von Microsoft vorgeschlagenen Mitigationsmaßnahmen (siehe oben) keine hinreichende Schutzwirkung entfalten. IT-Sicherheitsverantwortliche sollten daher **schnellstmöglich die Installation der am 8. November 2022 veröffentlichten Patches** (KB5019758) prüfen.

Links

Update 3:
[CROW2022] OWASSRF: CrowdStrike Identifies New Exploit Method for Exchange Bypassing ProxyNotShell Mitigations:
https://www.crowdstrike.com/blog/owassrf-exploit-analysis-and-recommendations/

[MSRC2022b] CVE-2022-41080 Microsoft Exchange Server Elevation of Privilege Vulnerability
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-41080

[MSRC2022c] CVE-2022-41082 Microsoft Exchange Server Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2022-41082

[GTSC2022] Exchange Zero-Day Exploit in-the-Wild:
https://gteltsc.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

[MSRC2022] Customer Guidance for Reported Zero-day Vulnerabilities in Microsoft Exchange Server:

https://msrc-blog.microsoft.com/2022/09/29/customer-guidance-for-reported-zero-day-vulnerabilities-in-microsoft-exchange-server/

[MSRC2022a] Control remote PowerShell access to Exchange servers:
https://learn.microsoft.com/en-us/powershell/exchange/control-remote-powershell-access-to-exchange-servers

[BSI2022] BSI IT-Grundschutz – OPS.1.1.3 Patch- undÄnderungsmanagement:
https://bsi.bund.de/dok/989196

[TWIT2022a] Twitter-Suchergebnisse zu "ProxyNotShell":
https://twitter.com/search?q=proxynotshell

[TWIT2022b] Twitter-Post von Will Dormann:
https://twitter.com/wdormann/status/1576922677675102208

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.