Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zimbra: Aktive Ausnutzung der Schwachstelle CVE-2024-45519

CSW-Nr. 2024-282632-10k2, Version 1.0, 02.10.2024

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:CLEAR: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten, die das TLP explizit nicht adressiert, dürfen Informationen der Stufe TLP:CLEAR 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 1.10.2024 wies das IT-Sicherheitsunternehmen Proofpoint darauf hin, dass seit kurzem Cyber-Angriffe auf die Kollaborationslösung Zimbra beobachtet würden [X2024]. Dabei fokussierten sich die Täter auf die Schwachstelle CVE-2024-45519, für die der Hersteller am 4. September einen Patch herausgegeben hatte [ZIMB2024]. Proofpoint führte weiter aus, dass die Angreifenden Mails an Zielsysteme verschicken, in denen das cc-Feld zur Einschleusung und Ausführung von schadhaftem Code genutzt werden soll. Für den Versand griffen die Täter dabei bislang auf (gefälschte) gmail-Adressen zurück.

Eine detaillierte Analyse der Schwachstelle steht auf der Webseite von Project Discovery [PrDi2024] zur Verfügung. Dort beschreiben die Autoren einerseits ausführlich, wie eine Ausnutzung ablaufen könnte, machen jedoch zeitgleich darauf aufmerksam, dass Angriffsversuche nur dann erfolgreich sind, wenn die postjournal-Funktion in Zimbra aktiviert ist.

Eine offizielle Bewertung für CVE-2024-45519 nach dem Common Vulnerability Scoring System (CVSS) liegt zum aktuellen Zeitpunkt nicht vor.

Bewertung

Mail- bzw. Kollaborationsanwendungen im Allgemeinen sind für die Prozesse in Organisationen von zentraler Bedeutung. Angreifende könnten Schwachstellen nutzen, um Betriebsabläufe zu stören, vertrauliche Informationen abzugreifen oder zu sabotieren.

* 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.

Zwar liegen bislang ausschließlich Berichte über Angriffsversuche mithilfe von gmail-Adressen vor, allerdings ist davon auszugehen, dass auch andere Mailanbieter für die Aktivitäten missbraucht werden – zumal durch die Veröffentlichung der Schwachstellendetails mit weiteren Attacken anderer Akteure zu rechnen ist.

Maßnahmen

IT-Sicherheitsverantwortliche sollten die vom Hersteller bereitgestellten Patches zeitnah installieren, um das Risiko einer Kompromittierung auszuschließen. Zimbra bietet in diesem Zusammenhang die aktualisierten Versionen:

- 9.0.0 Patch 41,
- 10.0.9,
- 10.1.1 und
- 8.8.15 Patch 46

an. Sofern die Updates nicht kurzfristig ausgerollt werden können, sollte überprüft werden, ob der postjournal-Dienst deaktiviert und die Liste vertrauenswürdiger Clients über die mynetworks-Komponente korrekt konfiguriert sind.

Project Discovery bietet darüber hinaus ein Skript für den Schwachstellen-Scanner Nuclei an, mit dessen Hilfe die eigene Betroffenheit überprüft werden kann [GITH2024].

Weitere Hinweise zur sicheren Nutzung von Mail- und Konfigurationsanwendungen finden sich im IT-Grundschutz des BSI [BSI2024a], [BSI2024b].

Links

[X2024] Tweet auf X:
https://x.com/threatinsight/status/1841089939905134793

[ZIMB2024] Zimbra Security Advisories:
https://wiki.zimbra.com/wiki/Zimbra_Security_Advisories

[PrDi2024] Zimbra - Remote Command Execution (CVE-2024-45519):
https://blog.projectdiscovery.io/zimbra-remote-code-execution/

[GITH2024] Zimbra Collaboration Suite < 9.0.0 - Remote Code Execution (CVE-2024-45519):
https://github.com/projectdiscovery/nuclei-templates/pull/10860

[BSI2024a] BSI IT-Grundschutz: APP.5.3 Allgemeiner E-Mail-Client und -Server:
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_5_3_Allgemeiner_E-Mail_Client_und_Server_Edition_2023.pdf

[BSI2024b] BSI IT-Grundschutz: APP.5.4 Unified Communications und Collaboration (UCC):
https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2023/06_APP_Anwendungen/APP_5_4_Unified_Communications_und_Collaboration_Edition_2023.pdf

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 vom BSI verwendete TLP basiert auf der Definition der TLP Version 2.0 des „Forum of Incident Response and Security Team“ (FIRST). Es dient der Schaffung von Vertrauen in Bezug auf den Schutz ausgetauschter Informationen durch Regelungen der Weitergabe. Eine unbefugte Weitergabe kann eine Verletzung der Vertraulichkeit, eine Rufschädigung, eine Beeinträchtigung der Geschäftstätigkeit oder datenschutzrechtliche Belange zur Folge haben. Im Zweifelsfall ist immer in Absprache mit dem Informationsersteller zu handeln.
2. Welche Einstufungen existieren?
   - **TLP:CLEAR: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:CLEAR ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden. Eine Weitergabe von den Partnerorganisationen an weitere Personen oder Organisationen ist solange zulässig, wie diese weiteren Empfänger derselben Nutzergruppe (bspw. Angehörige der Cybersecurity-Community) angehören.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Weitergabe**
     Der Empfänger darf die Informationen, welche als TLP:AMBER gekennzeichnet sind, an seine Partner weitergeben, soweit diese die Informationen zur Schadensreduktion oder dem eigenen Schutz benötigen. Eine Weitergabe von den Partnern an Dritte ist nicht erlaubt und auch innerhalb der Partnerorganisationen gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Informationsersteller kann weitergehende oder zusätzliche Einschränkungen der Informationsweitergabe festlegen. Diese müssen eingehalten werden.
     - **TLP:AMBER+STRICT: Eingeschränkte interne Weitergabe**
       Die Einstufung von Informationen als TLP:AMBER+STRICT beschränkt die Weitergabe ausschließlich auf die Organisation des Empfängers. Jegliche Weitergabe darüber hinaus ist untersagt. Es gilt „Kenntnis nur, wenn nötig“. 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. TLP:RED eingestufte Informationen sollten möglichst mündlich oder persönlich übergeben werden.
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:CLEAR eingestufte Informationen aus dem Kreis der Verpflichteten.

Hinweis zu Upload-, Prüf- und Übersetzungsdiensten

TLP-eingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.