Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Ungepatchte Schwachstellen im Mail Transfer Agent Exim

Nr. 2023-266613-1122, Version 1.1, 02.10.2023

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

Der Open Source Mail Transfer Agent (MTA) Exim weist mehrere schwerwiegende ungepatchte Schwachstellen auf. Besonders kritisch ist eine Buffer Overflow Schwachstelle in der SMTP-Implementierung, CVE-2023-42115 [ZDI23_a], die einer entfernten, unauthorisierten angreifenden Person gegebenenfalls das Ausführen von Code mit Rechten des Service Accounts, mit dem Exim betrieben wird, ermöglicht. Sie erreicht daher eine CVSS-Bewertung von 9.8 ("kritisch"). In Folge der Code-Ausführung könnte es Angreifenden unter anderem möglich sein, sensible Daten inkl. transportverschlüsselter E-Mails abfließen zu lassen.

Die Schwachstellen wurden im Juni 2022 an den Hersteller gemeldet und nach Ablauf des für die Entwicklung von Patches eingeräumten Zeitfensters durch die Zero Day Initiative am 27.9.2023 veröffentlicht,ohne dass Patches zur Verfügung stehen. Zur Zeit ist unbekannt, ob und wie die in Entwicklung befindliche Exim-Version 4.97 die Schwachstellen schließen wird.

Es scheinen ca. 3,5 Millionen Installationen des Open Source MTAs Exim über das Internet erreichbar zu sein, hiervon etwas über 190.000 in Deutschland.

Neben der besonders kritischen Schwachstelle wurden weitere nach CVSS "hoch" bewertete Schwachstellen durch die Zero Day Initiative veröffentlicht:

* 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.

CVE-2023-42116 - CVSS-Bewertung: 8.1 [ZDI23_b]

Durch unzureichende Prüfung von Grenzwerten beim Verarbeiten von NTLM-Challange Anfragen kann ebenfalls entfernten Angreifenden eine Code-Ausführung möglich sein.

CVE-2023-42117 - CVSS-Bewertung: 8.1 [ZDI23_c]

Es handelt sich hierbei ebenfalls um eine Schwachstelle im SMTP-Dienst, die entfernten Angreifenden durch spezielle Anfragen möglicherweise eine Code-Ausführung ermöglichen.

CVE-2023-42118 - CVSS-Bewertung: 7.5 [ZDI23_d]

Entfernte Angreifende könnten die Schwachstelle mit einer speziell präparierten Anfrage möglicherweise ausnutzen, um Code auszuführen. Die Schwachstelle wird durch einen Fehler in der Verarbeitung von SPF Makros hervorgerufen.

Update 1:
Mittlerweile wurden Sicherheitsupdates in einem geschützten Repository für die Distributoren von dem Hersteller veröffentlicht, welches die kritischen Schwachstellen [SECL23] behebt . **Die Versionen 4.96.1 und 4.97 beheben die Schwachstellen.** Zudem wurden vom Hersteller weitere Details bekannt gegeben, welche beschreiben, wie die Schwachstelle ausgenutzt werden kann [EXIM23].

Updates für die Distributionen selbst stehen noch aus, können aber zeitnah vom Distributor veröffentlicht werden.

Bewertung

Die Betroffenheit durch die Schwachstellen ist hoch. In Deutschland werden zehntausende SMTP-Server mit der Software Exim betrieben und sind entsprechend durch die Schwachstelle gefährdet.

Aktuell sind keine technischen Details oder ein Proof-of-Concept öffentlich verfügbar, jedoch wurden ähnliche Schwachstellen in Exim in der Vergangenheit zeitnah ausgenutzt.

Maßnahmen

Mitigation:

IT-Sicherheitsverantwortliche sollten regelmäßig **auf verfügbare Updates für Exim prüfen** und diese so bald verfügbar installieren.

Für die Zeit, bis ein Patch zur Verfügung steht, kann auch der Wechsel auf einen anderen SMTP-Mailserver bzw. Mail Transfer Agent (MTA) erwogen werden, wenn Verfügbarkeitsanforderungen andere Mitigationsmaßnahmen nicht zulassen.

Update 1:
Durch die Verfügbarkeit von Patches und Mitigationsmaßnahmen für die offenen Schwachstellen, können die mit einem Sicherheitsupdate versehenen Versionen 4.96.1 und 4.97 von Exim wieder eingesetzt werden. Auch durch getroffene Mitigationsmaßnahmen kann Exim weiterverwendet werden.

Zur Verfügung stehende **Mitigationsmaßnahmen** [EXIM23]:

- CVE-2023-42114 und CVE-2023-42116 betreffen die Komponente "SPA auth" und können mitigiert werden, indem keine SPA (NTLM) Authentifikation genutzt wird.
- CVE-2023-42115 betrifft die Komponente "EXTERNAL auth" und kann mitigiert werden, indem die externe Authentifikation deaktiviert wird.

Detektion:

Des Weiteren sollten die mit Exim betriebenen Server besonders beobachtet werden. Bei der Ausnutzung *zurückliegender* Schwachstellen waren u. a. folgende Anomalien zu beobachten:

- Unerwartete ausgehende HTTP-Verbindungen (zu Nachladeservern der Angreifer)
- Anlegen neuer Dateien in den aus dem Internet erreichbaren Webserver-Verzeichnissen (z. B. PHP-Webshells)
- Unerwartete eingehende HTTP(S)-Verbindungen (z. B. auf PHP-Webshells der Angreifer)
- Existenz neuer Accounts (vgl. [NSA20])
- Existenz neuer SSH-Keys (vgl. [NSA20])
- Änderungen an der EXIM-Konfiguration, insbesondere zu Sicherheitseigenschaften (vgl. [NSA20])

Darüber hinaus ist im Fall einer Kompromittierung mit der Exfiltration größerer Email-/Datenmengen zu rechnen, was sich im Monitoring bemerkbar machen dürfte.

Im Falle der Detektion eines Angriffs oder einer Exfiltration sollte das betreffende System offline genommen werden, sofern die Verfügbarkeitsanforderungen dies zulassen.

Das BSI bittet darum, Auffälligkeiten im Zusammenhang mit einer möglichen Exim-Server Kompromittierung an das BSI-Lagezentrum oder CERT-Bund zu melden.

Links

[ZDI23_a] https://www.zerodayinitiative.com/advisories/ZDI-23-1469/

[ZDI23_b] https://www.zerodayinitiative.com/advisories/ZDI-23-1470/

[ZDI23_c] https://www.zerodayinitiative.com/advisories/ZDI-23-1471/

[ZDI23_d] https://www.zerodayinitiative.com/advisories/ZDI-23-1472/

[NSA20] National Security Agency, "SANDWORM ACTORS EXPLOITING VULNERABILITY IN EXIM MAIL TRANSFER AGENT", 28.05.2020

https://media.defense.gov/2020/May/28/2002306626/-1/-1/0/CSA%20Sandworm%20Actors%20Exploiting%20Vulnerability%20in%20Exim%20Transfer%20Agent%2020200528.pdf

Update 1:

[SECL23] https://seclists.org/oss-sec/2023/q3/254

[EXIM23] https://lists.exim.org/lurker/message/20231001.165119.aa8c29f9.en.html

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.