



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Schwachstellen in Exim bedrohen Unix-Mailserver

CSW-Nr. 2021-216469-1032, Version 1.0, 05.05.2021

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

Das Sicherheitsunternehmen Qualys veröffentlichte am 4. Mai 2021 einen Bericht über die Entdeckung von insgesamt 21 Schwachstellen in der Anwendung Exim (Experimental Internet Mailer) [Qua2021]. Hierbei handelt es sich um einen Mail-Transfer-Agent (MTA), der weltweit auf ca. 4 Millionen E-Mailservern mit Unix-Betriebssystem zum Einsatz kommt. In einigen Distributionen ist Exim bereits vorab enthalten – hierunter zum Beispiel das weit verbreitete Debian.

Entsprechend der Anzahl der gefundenen Sicherheitslücken nennt Qualys die Entdeckung „21Nails“: Zehn Bedrohungen können aus der Ferne ausgenutzt werden (CVE-2020-28017 bis CVE-2020-28026), elf Sicherheitslücken erfordern lokalen Zugriff durch den Angreifer (CVE-2020-28007 bis CVE-2020-28016 sowie CVE-2021-27216). Je nach Schwachstelle reicht die Auswahl der betroffenen Exim-Versionen zurück bis ins Jahr 2004.

Bei einem Angriff können nicht nur Informationen abgegriffen, sondern sogar Root-Rechte auf dem Server erlangt werden.

* 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

Aufgrund der ständigen Erreichbarkeit von MTAs aus dem Internet und der zahlreichen Bedrohungsszenarien durch und mit E-Mails stellt der vorliegende Sachverhalt eine signifikante Gefährdung für Organisationen dar. Es können nicht nur Informationen abgegriffen, sondern auch Kommunikationsinhalte sabotiert werden (Veränderung von Nachrichten, Verteilung von maliziösen Anhängen). Darüber hinaus ist auch die weitere Kompromittierung des Netzwerks einer Organisation denkbar.

Maßnahmen

Als Herausgeber hat die Universität von Cambridge Exim in der Version 4.94.2 veröffentlicht [Exi2021]. Hier sind alle genannten Schwachstellen behoben.

Das BSI rät dazu, das Update kurzfristig auf allen betroffenen Mailservern auszurollen und hierfür entweder die Pakete der jeweiligen Linux-Distribution zu verwenden oder über ein Repository die Version exim-4.94.2 zu installieren. Empfehlungen zum Vorgehen, falls eine Version < v 4.94 eingesetzt wird, finden sich unter [OSS2021].

Weitere Informationen zum sicheren Betrieb von E-Mail-Diensten stellt das BSI unter [BSI2021] bereit.

Links

[QUA2021] 21Nails: Multiple Critical Vulnerabilities in Exim Mail Server

<https://blog.qualys.com/vulnerabilities-research/2021/05/04/21nails-multiple-vulnerabilities-in-exim-mail-server>

[Exi2021] Latest Version: 4.94.2

<https://www.exim.org/>

[OSS2021] Exim 4.94.2 - security update released

<https://www.openwall.com/lists/oss-security/2021/05/04/6>

[BSI2021] APP.5.3: Allgemeiner E-Mail-Client und -Server (Edition 2021)

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompodium Einzel PDFs 2021/06 APP Anwendungen/APP 5 3 Allgemeiner E-Mail Client und Server Edition 2021.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 TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensiblen 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.