heise Security

Mail-Verschlüsselung: Überprüfung von Enigmail fördert kritische Lücken zutage UPDATE

Alert! 20.12.2017 14:44 Uhr
Dennis Schirrmacher

(Bild: pixabay)

Pentester haben sich Thunderbird und Enigmail zum verschlüsselten Versenden von E-Mails angeschaut und kritische Schwachstellen entdeckt. Davon sind noch nicht alle geschlossen.

Enigmail und Thunderbird sind verwundbar. Über das Duo kann man via PGP verschlüsselte E-Mails versenden. Setzen Angreifer an den zum Teil als kritisch eingestuften Schwachstellen an, könnten sie, wenn die Voraussetzungen stimmen, unter anderem Mails entschlüsseln.

Davor **warnen Sicherheitsforscher[1]** von Cure53. Sie haben sich Thunderbird und Enigmail im Zuge eines Audits angeschaut. Diese Überprüfung haben der E-Mail-Anbieter Posteo und Mozillas Open Source Fund (MOSS) finanziert.

Bisher sind nur Infos zu den Lücken in Enigmail bekannt, da die Entwickler diese bereits in der **Version 1.9.9[2]** geschlossen haben. Die Schwachstellen in Thunderbird sind offenbar noch offen.

Identitätsklau hoch zwei

Den Bedrohungsgrad von zwei Lücken in Enigmail stufen die Sicherheitsforscher als "kritisch" ein. Setzen Angreifer an einer der Lücken an, können sie Enigmail dazu zwingen, einen beliebigen öffentlichen PGP-Schlüssel zu akzeptieren, der beispielsweise zum privaten Schlüssel eines Angreifers passt.

So könnten Angreifer sich als jemand anderes ausgeben und mit dem eigenen Schlüssel signierte und verschlüsselte Mails unter falschem Namen verschicken – für den Empfänger sieht alles in Ordnung aus. Allerdings geht das nur, wenn Opfer A schon eine Mail an Opfer B geschrieben hat, die der Angreifer unterwegs abfangen und manipulieren kann. Die Lücke könnten Betrüger etwa zur Spionage missbrauchen

Über die zweite kritische Schwachstelle könnten Angreifer fremde Signaturen von Opfern klauen und für eigene Mails nutzen. Für den Empfänger sieht es so aus, als wäre die Mail vom Opfer signiert. Dafür muss ein Angreifer lediglich eine vom Opfer signierte Mail als Anhang in eine neue Mail packen und diese verschicken, erläutern die Sicherheitsforscher.

Mails im Klartext

Nutzen Angreifer eine mit dem Bedrohungsgrad "hoch" eingestufte Lücke aus, können sie unter gewissen Umständen Mails entschlüsseln. Dafür müsste ein Angreifer jedoch unter anderem verschlüsselten E-Mail-Verkehr mitschneiden und Mails manipulieren können. Weitere Voraussetzungen und Details dazu beschreiben die Sicherheitsforscher in ihrer **Warnung[3]**.

Schwächen von Thunderbird

Mittlerweile hat Posteo im Rahmen eines Sicherheitshinweises **weitere Ergebnisse des Sicherheits-Audits[4]** veröffentlicht. Unter anderem geht daraus die Gesamtzahl der gefundenen Schwachstellen – nämlich 22 – hervor. Drei davon stuften die Tester als "kritisch", fünf als "hoch" ein.

Laut Posteo offenbarte das Audit neben den Gefahren der Thunderbird-Enigmail-Kombo auch grundlegende Schwächen in der Add-on-Architektur des Mail-Clients. Infolge einer unzureichenden Abgrenzung der Add-ons voneinander könnten Angreifer mittels kompromittierter Erweiterungen auf (sensible) Inhalte im Mail-Client zugreifen.

RSS-Feeds als Gefahr

Auch die Verwendung von RSS-Feeds in Thunderbird ist dem E-Mail-Anbieter zufolge derzeit mit hohen Sicherheitsrisiken verbunden. Sie könne "die Vertraulichkeit der Ende-

zu-Ende-verschlüsselten Kommunikation" in Thunderbird gefährden.

Da die Beseitigung der RSS-Schwachstellen laut Posteo möglicherweise erst in Thunderbird Version 59 abgeschlossen sein wird, rät das Unternehmen bis auf weiteres dringend von der Feed-Nutzung in Thunderbird ab. Bis zur Verbesserung der Add-on-Architektur sei es zudem sinnvoll, entweder vollständig auf Erweiterungen zu verzichten oder zumindest besonders sorgfältig auf deren Herkunft und Vertrauenswürdigkeit zu achten. Weitere Informationen zum Audit, Sicherheitshinweise sowie Statetements der involvierten Unternehmen sind Posteos **Webseite[5]** zu entnehmen.

[UPDATE, 20.12.2017 18:10 Uhr]: Die Meldung wurde um Informationen aus einem aktuellen Blogeintrag von Posteo erweitert.

[UPDATE, 21.12.2017 08:50 Uhr]

Beteiligte am Audit im Fließtext korrigiert. (**des[6]**)

URL dieses Artikels:
`http://www.heise.de/-3924138`

Links in diesem Artikel:
[1] https://enigmail.net/download/other/Enigmail%20Pentest%20Report%20by%20Cure53%20-%20Excerpt.pdf
[2] https://www.enigmail.net/index.php/en/download/changelog
[3] https://enigmail.net/download/other/Enigmail%20Pentest%20Report%20by%20Cure53%20-%20Excerpt.pdf
[4] https://posteo.de/blog/sicherheits-warnung-f%C3%BCr-thunderbird-und-enigmail-nutzer-schwachstellen-gef%C3%A4hrden-vertraulichkeit-der-kommunikation
[5] https://posteo.de/blog/sicherheits-warnung-f%C3%BCr-thunderbird-und-enigmail-nutzer-schwachstellen-gef%C3%A4hrden-vertraulichkeit-der-kommunikation
[6] mailto:des@heise.de