Riseup läßt Sicherheitslücke offen

von: eLBe am: 30.09.2018 - 21:46
Themen: Netactivism

Das Management von Riseup schafft es derzeit nicht, eine Sicherheitslücke zu schließen, welche es einem Angreifer ermöglicht die Emails von Riseup-Nutzern zu manipulieren während sie verfasst werden. Das Problem betrifft die Möglichkeit der Mehrfachanmeldung, welche nicht nur Nutzern ermöglicht mehr als eine Anmeldung gleichzeitig durchzuführen, zu welchem Zweck auch immer, sondern auch eine bestimmte Art Angreifer dazu ermächtigt sich in die Zusammenstellung von Emails auf eine Weise einzumischen, welche nicht unmittelbar als Missbrauch durch Dritte erkennbar ist. Durch die Möglichkeit der Mehrfachanmeldung könnte ein TBTFBF-Angreifer mit der Fähigkeit Passwörter zu stehlen Verständigungsfehler herbeiführen, die stattdessen als Unachtsamkeit des Nutzers erscheinen, und so Verwirrung und Verstörung sowohl beim Absender als auch beim Empfänger verursachen; sowie im schlimmsten Fall den Verlust von wichtigen Inhalten ohne eindeutige Spuren wodurch dieser entstanden ist. So könnte etwa in einer Email an einen Anwalt ein Dokument für ein Gericht verlorengehen, und ein Auftrag nicht fristgemäß ausgeführt werden; und im schlimmsten Fall würde ein Riseup-Nutzer vermuten selbst eine Nachlässigkeit begangen zu haben.

Selbstverständlich könnte dieselbe Art Angreifer mit einem gestohlenen Passwort auch eine ganze Email im Namen des Riseup-Nutzers total fälschen, doch da dies sofort als Manipulation auffallen würde, würde der Nutzer vermutlich am nächsten Tag mit einem Ausdruck davon zu einem Anwalt gehen, und der Angriff würde auffliegen. Daher ist der unscheinbare Angriff für den TBTFBF (too big to fail brute force) attacker, den gewaltmonopolistischen Angreifer, sehr viel attraktiver als der offen erkennbare Angriff, da er theoretisch auf eine beliebige Dauer ausgedehnt werden kann, die nur von der Achtsamkeit, dem Selbstvertrauen und dem technischen Verständnis des jeweiligen Nutzers abhängt. Das ist auch der Grund warum die Möglichkeit der Mehrfachanmeldung so gefährlich ist, da sie Angriffe nicht nur gegen die Wahrheit und die Echtheit ermöglicht, sondern auch solche gegen das Vertrauen und die Achtsamkeit. Und sie ist noch gefährlicher in Kombination mit der Riseup-Linie vollkommenen Verzichts auf Verhaltensüberwachung, da ohne Verhaltensdaten keine Spuren hinterlassen werden. Riseup verzichtet auf Verhaltensdaten um Nutzer gegen Beweissicherung zu schützen, welche gegen sie missbraucht werden könnte, doch wenn es eine offene Sicherheitslücke gibt, dann schützt diese Linie auch Angreifer, was bedeutet, dass das Schließen von Sicherheitslücken dementsprechend wichtiger ist um eine ansonsten gutartige Linie zu rechtfertigen. Klassisches Beispiel, wenn eine Türe gezielt ohne Überwachungskamera bleibt, dann ist es um so wichtiger Türsiegel zu benutzen um unrechtmäßige Zugriffe mithilfe von Schlüsselkopien auszuschließen.

Das Management von Riseup wurde am Dienstag den 25.9. um 22:00 hiesiger Zeit in Kenntnis gesetzt, und bestätigte noch am selben Tag die Kenntnisnahme, doch hat bislang nichts unternommen um das Problem zu beheben. Stattdessen forderte mich ein offensichtlich hilfloser und weitgehend ratloser Riseup-Manager dazu auf, seine Arbeit für ihn zu erledigen. Als ich ihm antwortete, dass ich gerade nicht die erforderlichen Arbeitsmittel verfügbar hätte, wurde er wortkarg und zeigte kein weiteres Interesse das Problem zu lösen. Die Sicherheitslücke kam auf den Tisch, als ich mich von Experten beraten ließ wie Riseup-Postfächer sicherer gemacht werden können ohne die derzeitige Linie zu ändern, nachdem ich obige Beweise für Manipulationen gesichert hatte. Technisch ist es auch ohne Verhaltensüberwachung möglich mittels einer Siegel-Kennung nachzuvollziehen dass zwischen zwei legitimen Sitzungen keine illegitime Anmeldung stattgefunden hat. Detaillierte technische Beschreibungen, wie eine Zugangs-Versiegelung mittels kryptographischer Standard-Funktionen umgesetzt werden kann, wurden mittels Expertenunterstützung dem Riseup-Management kostenfrei bereitgestellt, doch ohne Ergebnis. Da die Riseup-Linie kein Vergessen von Passwörtern erlaubt, ist ein Wechsel des Passworts auch keine geeignete Lösung gegen einen TBTFBF-Angreifer mit der Fähigkeit Passwörter zu stehlen.

Vollständige Debatte mit allen technischen Einzelheiten (nur für Riseup-Nutzer):
https://support.riseup.net/en/ticket/9515-imap-access-log-file-availability

Siehe auch: https://tinyurl.com/problem-der-nachrichtendienste

Danke für Expertenberatung an den Chaos Computer Club: https://www.ccc.de/

Siehe auch: Riseup Übersetzungsgruppe: Unzensierte Version des letzten Riseup-Rundschreibens:
https://de.indymedia.org/node/24763

Englischsprachige Ausgabe dieses Artikels:

https://nyc.indymedia.org/en/2018/09/127423.html
https://www.indybay.org/newsitems/2018/09/29/18817886.php
http://boston.indymedia.org/newswire/display/227196/index.php

Bilder:

webadresse:
https://tinyurl.com/lb-ar...
Lizenz des Artikels und aller eingebetteten Medien:
Creative Commons by-sa: Weitergabe unter gleichen Bedingungen

Neue Ergänzung schreiben Verstoß gegen Moderationskriterien melden

Ergänzungen

Panik!

Von: tastytea am: 01.10. - 12:23

Der bugreport ist nicht (mehr?) aufrufbar. Das problem tritt nur auf, wenn dem angreifenden das passwort bekannt ist; zu dem zeitpunkt fällt der "bug" eh nicht ins gewicht, da der gesamte account kompromittiert ist. Entgegen der behauptung im artikel gibt es sehr wohl die möglichkeit, dass passwort zu ändern: https://riseup.net/en/email/settings/mail-passwords

Schließlich sei noch anzumerken, dass eine woche eine sehr kurze frist für einen bugfix ist, besonders da es sich um ein ehrenamtliches projekt handelt. Üblich ist, nach dem bugreport dem prokekt 3 monate zeit zu lassen, bevor die panikglocke geläutet wird.

Verstoß gegen Moderationskriterien melden

@tastytea

Von: eLBe am: 02.10. - 13:42

Das Helpticket ist nach wie vor zugänglich, allerdings nur für angemeldete Riseup-Nutzer. Falls es nicht direkt klappt erst beim Support anmelden und dann den Deeplink klicken.

Dass Passwörter nicht geändert werden könnten wurde nicht behauptet, sondern dass ein Vergessen von Passwörtern nicht toleriert wird. Ungünstigstenfalls sperrt man mit einer Passwortänderung nur sich selber aus nicht aber einen TBTFBF-Angreifer. Warum das Gesamtkompromittierungsargument nicht greift wurde bereits im Artikel erörtert.

Anlass zur Panik besteht grundsätzlich nicht, sondern zu Skepsis, Achtsamkeit und Wachsamkeit. Die oben beschriebe Problematik wurde schon länger beobachtet, jetzt aber erstmalig öffentlich nachvollziehbar dokumentiert. Ein Grund länger abzuwarten damit an die Öffentlichkeit zu gehen bestand nicht, und es hatte auch niemand von Riseup um einen bestimmten Aufschub gebeten. Zweck der Öffentlichmachung ist es zeitnah Abhilfe zu erwirken.

Verstoß gegen Moderationskriterien melden

@eLBe

Von: tastytea am: 02.10. - 14:49

Nochmal: Wenn der angreifende vollzugriff auf den account hat, ist es zu spät. Dieser zusätzliche bug fällt kaum ins gewicht.

Der einzige wirksame schutz sind mathematisch sichere passwörter und verschlüsselungsverfahren. Den bug zu fixen ist zwar wünschenswert, läuft aber auf einen neuanstrich einer abgebrannten hütte heraus.

Verstoß gegen Moderationskriterien melden

Das mit dem Passwort müsste

Von: alf am: 04.10. - 16:40

Das mit dem Passwort müsste noch mal genauer erklärt werden, normalereweise hat man immer verkackt wenn jemand auf das Passwort kommt. wer ist der TBTFBF-Angreifer? Meint das jemanden mit riesigen Rechner- und Netzwerkkapazitäten? Passwörter brutforcen wird normalerweise dadurch verhindert, dass nach mehrmaliger Fehleingabe die Intervalle zwoschen den möglichen Versuchen immer länger werden. Ist das bei Riseup nicht gegeben? Das wäre allerdings ein Problem. Ansonsten gelten die üblichen Regeln zur Passwortsicherheit: sehr lang, quasizufällige Folgen von Buchstaben, Ziffern und Sonderzeichen, die kein in irgendeiner Sprache gültiges Wort enthalten. Bei z.B. 100 solchen Zeichen kommt auch die NSA mit ihrer Computerpower nicht per Brutforce gegen an.

Verstoß gegen Moderationskriterien melden

@ 02.10. - 14:49

Von: eLBe am: 22.10. - 19:23

Von: eLBe am: 22.10. - 17:01

Von: eLBe am: 05.10. - 14:05

@ 02.10. - 14:49

Ein TBTFBF-Angreifer (too big to fail brute force / zu mächtig zum Aufgeben und mit brutaler Gewalt) kontrolliert theoretisch das gesamte Internet und kann also auch das neue, geänderte Passwort herausbekommen. Hinzu kommt die Gefahr vielleicht das geänderte Passwort zu vergessen.

Der einzig nachhaltige Schutz dagegen ist außerhalb des Internet alles dafür zu tun dass es diese Art Angreifer nicht mehr geben kann. Wie gesagt, die Panik sollten wir den Provokateuren von BND, BfV, etc. überlassen, die haben gute Gründe dafür. Dein Vergleich ist daher Quatsch, es ist eher wie eine sorgfältige Ladeninventur nach einer Lebensmittelerpressung. Wer Gift in Kleinkindernahrung mischt, der zündet nicht den Einkaufsmarkt an, sonst wird sein Köder ja von niemandem mehr arglos geschluckt.

Siehe auch den Link zum Problem der Nachrichtendienste.

Bilder:

Verstoß gegen Moderationskriterien melden

@ 04.10. - 16:40

Von: eLBe am: 22.10. - 19:26

Von: eLBe am: 22.10. - 17:05

Von: eLBe am: 05.10. - 14:08

@ 04.10. - 16:40

Im Prinzip ja, aber brutale Gewalt beinhaltet bspw. auch den Raum in dem Deine Tastatur klackert mit einer Abhörwanze zu belauschen, oder die Chipkarte mit Deinem unknackbaren Schlüssel aus der Schreibtischschublade zu stehlen während Du Frühstück einkaufen bist.

Wie im Artikel betont, diese Art Angreifer will möglichst lange manipulieren ohne bemerkt zu werden. Ein Motiv Dein Haus anzuzünden hat diese Art Angreifer daher erst dann, wenn sowieso gerade ein Atomunfall, ein Militärputsch oder ein Pogrom stattfindet, und der Rest der Welt woandershin guckt.

Bilder:

Verstoß gegen Moderationskriterien melden