



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Backdoor in XZ für Linux

Nr. 2024-223608-1022, Version 1.0, 30.03.2024

IT-Bedrohungslage*: **3 / Orange**

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 Anbieter Red Hat hat am 29.03.2024 bekannt gegeben, dass in den Versionen 5.6.0 und 5.6.1 der "xz"-Tools und -Bibliotheken maliziöser Code entdeckt wurde, der es ermöglicht, die Authentifizierung in sshd über systemd zu umgehen. Der Schwachstelle wurde als CVE-2024-3094 veröffentlicht.

Die Injektion, die in den xz-Versionen 5.6.0 und 5.6.1 enthalten ist, ist verschleiert und nur im Download-Paket vollständig enthalten - in der Git-Distribution fehlt lediglich das Makro, welches die Erstellung des Schadcodes auslöst. Dieser agiert dann mit sshd, dem Service, der dem Nutzer Zugang zum System mit Hilfe des SSH Protokolls gewährt.

Bisher sind innerhalb der Red Hat-Familie nur Fedora 41 und Fedora Rawhide betroffen. Es sind keine Versionen von Red Hat Enterprise Linux (RHEL) betroffen. Es besteht jedoch die Möglichkeit, dass auch andere Distributionen betroffen sein könnten.

Bewertung

Bei xz handelt sich um ein universelles Datenkomprimierungsformat, das in fast jeder Linux-Distribution enthalten ist, sowohl in Gemeinschaftsprojekten als auch in kommerziellen Produktdistributionen. Im Wesentlichen hilft es bei der Komprimierung (und anschließenden Dekomprimierung) großer Dateiformate in kleinere, besser handhabbare Größen für die gemeinsame Nutzung durch Dateiübertragung.

Details zur Ausnutzung sowie ein Proof-of-Concept sind bisher nicht bekannt. Der SSH-Daemon ist nicht direkt mit der manipulierten Bibliothek verbunden, nutzt jedoch systemd für die Authentifizierung,

* 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.

welches wiederum xz Komponenten verwendet. Durch den beinahe auf allen Linux-Servern eingesetzten SSH-Daemon und die in den letzten Jahren zunehmend eingesetzten systemd-Dienst, sind potentiell sehr viele Server im Internet von der Lücke betroffen. Allerdings dürften noch nicht viele Distributionen auf die relativ neuen und verwundbaren xz Versionen aktualisiert haben.

Genaue Informationen, wie es zur Kompromittierung und Bereitstellung manipulierter Versionen kommen konnte, sind bisher nicht öffentlich bekannt bzw. bestätigt.

Maßnahmen

IT-Sicherheitsverantwortliche sollten die Nutzung von Fedora 41 und Fedora Rawhide unverzüglich stoppen. xz selbst sollte auf eine ältere, stabile Version wie 5.4.6 zurückgesetzt werden. SUSE hat ein Downgrade-Verfahren veröffentlicht.

Auch bei Verwendung anderer Distributionen wird empfohlen, das Upgrade auf die xz Versionen 5.6.x nicht vorzunehmen bzw. wieder auf die sicheren Versionen zurück zu gehen.

Links

[01] Red Hat Security Alert, <https://www.redhat.com/en/blog/urgent-security-alert-fedora-41-and-rawhide-users>

[02] CISA Alert, <https://www.cisa.gov/news-events/alerts/2024/03/29/reported-supply-chain-compromise-affecting-xz-utils-data-compression-library-cve-2024-3094>

[03] SUSE Downgrade von xz, <https://build.opensuse.org/request/show/1163302>

[04] Diskussion zur Backdoor, <https://gist.github.com/thesamesam/223949d5a074ebc3dce9ee78baad9e27>

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.