Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum
BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

CrushFTP: Ausgenutzte Schwachstelle ermöglicht Datenabfluss

CSW-Nr. 2024-232029-1132, Version 1.1, 29.04.2024

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

Am 19. April 2024 warnte CrushFTP seine Kunden vor einer Schwachstelle in seiner gleichnamigen Dateiübertragungssoftware. Demnach könnte es Angreifenden gelingen, aus dem virtuellen Dateisystem (VFS) auszubrechen und Systemdateien herunterzuladen [CRUS24a]. Angreifende könnten daher an vertrauliche Daten auf dem Server gelangen.

Betroffen sind alle Produktversionen, sofern diese nicht auf CrushFTP 10.7.1 oder 11.1.0 aktualisiert wurden. Kunden die einen DMZ Server [CRUS24b] vor der CrushFTP Instanz einsetzen, sollen nach neuem Stand vom 22. April ebenfalls nicht vollständig geschützt sein.

Die Schwachstelle mit der Kennung CVE-2024-4040 wurde mit einem CVSS-Score von 7.7 bewertet und gefährdet alle CrushFTP Instanzen mit exponierten Webinterface Port. Der Hersteller konnte dem BSI jedoch bestätigen, dass die Schwachstelle auch von **nicht authentifizierten Angreifenden ausgenutzt werden kann**, was die Kritikalität deutlich erhöht.

Das Cyber-Sicherheitsunternehmen CrowdStrike berichtete auf Reddit über erste, vermutlich politisch motivierte zielgerichtete Angriffe mit dieser Schwachstelle [REDD24]. Der Hersteller teilte dem BSI mit, dass derzeit automatisierte Scans sowie eine breite aktive Ausnutzung stattfinden.

Update 1:

Nach Erkenntnissen von Sicherheitsforschenden des Unternehmens Rapid7 ist es möglich, dass Angreifende die komplette Kontrolle über einen verwundbaren CrushFTP Server erlangen können [RAPD24]. Ein Proof-of-Concept Exploit sowie technische Details zur Schwachstelle sind inzwischen

* 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.

öffentlich verfügbar. Gleichzeitig befinden sich in Deutschland nach Untersuchungen der Shadowserver Foundation noch über 90 verwundbare CrushFTP Server (Stand 28.04.2024) [SHAD24].

Bewertung

Die Schwachstelle stellt eine massive Bedrohung für die Vertraulichkeit der Daten einer Institution dar. Aufgrund von aktuellen Berichten über bereits stattgefundene Ausnutzungen könnte darüber hinaus bereits eine Exfiltration von Daten stattgefunden haben. Dass nicht authentifizierte Angreifende ebenso die Schwachstelle ausnutzen können und die DMZ keinen ausreichenden Schutz bietet, erhöht die Gefährdung deutlich.

Es findet eine breite Ausnutzung ungepatchter CrushFTP Instanzen statt. Ein schnelles Absichern der Systeme ist daher dringend notwendig.

Update 1:

Die Möglichkeit der kompletten Übernahme des Servers durch Angreifende verschärft – besonders im Hinblick auf die noch hohe Anzahl ungepatchter Systeme und die erschwerte Detektion einer Kompromittierung – das Schadenpotential.

Maßnahmen

IT-Sicherheitsverantwortliche sollten schnellstmöglich auf die absichernden Versionen 10.7.1 oder 11.1.0 von CrushFTP aktualisieren. Auch Kunden die eine DMZ einsetzen, sollten zeitnah auf eine absichernde Version aktualisieren, da die DMZ allein laut Hersteller langfristig nicht vollständig vor Angriffen schützt [CRUS24a].

Der Hersteller stellt eine Anleitung, wie ein Update in der Weboberfläche gestartet werden kann, unter [CRUS24a] zur Verfügung. Ebenso wird auf der Seite erklärt, wie im Falle eines Problems ein Backup eingespielt werden kann.

Aufgrund der möglicherweise stattgefunden Ausnutzung sollten nach der Aktualisierung vorsichtshalber alle Zugangsdaten auf dem System ausgetauscht werden, insbesondere diejenigen von Admin-Nutzern (wie "crushadmin"). IT-Sicherheitsbeauftragte sollten das Hashen von gespeicherten Passwörter aktivieren, um einen Abfluss von ungehashten Passwörtern zu verhindern [CRUS24c]. Sofern möglich (Enterprise Lizenz notwendig) sollte außerdem die Multi-Faktor Authentifizierung aktiviert werden [CURS24d].

Der Hersteller gibt an, dass es kaum möglich ist, sicher eine Ausnutzung festzustellen. Logeinträge die "<INCLUDE" beinhalten, können jedoch einen Indikator darstellen [CRUS24a].

Update 1:

Neben dem Patchen können IT-Sicherheitsverantwortliche ihre CrushFTP Server nach Empfehlungen von Rapid7 zusätzlich durch eine Aktivierung des Limitierten Server Modus mit den restriktivsten Einstellungen vor Angriffen mit Codeausführung auf der Administrator-Ebene härten. Organisationen sollten, sofern möglich, Firewalls vor CrushFTP Dienste schalten und den Zugriff auf diese nur von vertrauenswürdigen IP-Adressen erlauben. [RAPD24]

IT-Sicherheitsverantwortlichen wird empfohlen, sofern nicht bereits geschehen, auf verdächtige Logs zu prüfen. Auf AttackerKB [ATTA24] wurden in diesem Zusammenhang Indikatoren, die auf eine Kompromittierung hindeuten, neben Details zur Schwachstelle veröffentlicht.

Das BSI sendet mittlerweile über CERT-Bund Reports Benachrichtigungen an Betreiber verwundbarer CrushFTP Server. Dies entbindet IT-Sicherheitsverantwortliche jedoch nicht von ihren Verantwortungen im Rahmen des Patchmanagements.

Links

[CRUS24a] CrushFTP v11 – Update:
https://www.crushftp.com/crush11wiki/Wiki.jsp?page=Update

[CRUS24b] CrushFTP v11 – DMZ:
https://www.crushftp.com/crush11wiki/Wiki.jsp?page=DMZ

[CRUS24c] CrushFTP – Encryption:
https://www.crushftp.com/crush10wiki/Wiki.jsp?page=Encryption

[CURS24d] CrushFTP – OTP:
https://www.crushftp.com/crush10wiki/Wiki.jsp?page=OTP%20Settings

[REDD24] SITUATIONAL AWARENESS // 2024-04-19 // CrushFTP Virtual Filesystem Escape Vulnerability in the Wild:
https://www.reddit.com/r/crowdstrike/comments/1c88788/situational_awareness_20240419_crushftp_virtual/?rdt=35279

Update 1:

[RAPD24] Rapid7 – Unauthenticated CrushFTP Zero-Day Enables Complete Server Compromise
https://www.rapid7.com/blog/post/2024/04/23/etr-unauthenticated-crushftp-zero-day-enables-complete-server-compromise/

[SHAD24] Shadowserver Dashboard – CVE-2024-4040
https://dashboard.shadowserver.org/statistics/combined/tree/?day=2024-04-28&source=http_vulnerable&source=http_vulnerable6&tag=cve-2024-4040%2B&geo=all&data_set=count&scale=log

[ATTA24] AttackerKB – CVE-2024-4040
https://attackerkb.com/topics/20oYjlmfXa/cve-2024-4040/rapid7-analysis

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.