Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle mit Proof-of-Concept Exploit in Ghostscript

CSW-Nr. 2023-248889-1012, Version 1.0, 14.07.2023

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 11. Juli 2023 wurde zu einer kritischen Schwachstelle in der Open-Source PDF Bibliothek Ghostscript ein Proof-of-Concept Exploit veröffentlicht [KRO2023]. Die Schwachstelle mit der CVE-Nummer CVE-2023-36664 und einer CVSS-Bewertung von 9.8 ("kritisch") ermöglicht einem entfernten Angreifer die Ausführung von Remote Code. Die Schwachstelle wird durch eine fehlerhafte Berechtigungsvalidierung für Pipe-Geräte (mit dem Präfix "%pipe%" oder dem Pipe-Zeichen "|") verursacht.

Ghostscript, ein Interpreter für die PostScript-Sprache und PDF-Dateien, ist Teil vieler Distributionen als Standardinstallation. Obwohl Ghostscript selten direkt genutzt wird, wird es häufig von anderen Open-Source-Softwarepaketen zur Unterstützung von Druck- oder Konvertierungsvorgängen verwendet. Es ist eine erforderliche Abhängigkeit für "cups-filters", das ein Kernbestandteil des Common Unix Printing System (CUPS) ist, dem primären Mechanismus von Linux zum Drucken und für Druckdienste. Andere Anwendungen verwenden Ghostscript zum Lesen und Speichern von PostScript (PS), eingebettetem PostScript (EPS) oder PDF-Dateien. Auf einem Debian 12 System hängen 131 Pakete von Ghostscript ab. Die Liste der Anwendungen, die Ghostscript verwenden, umfasst namhafte Desktop- und Produktivanwendungen wie LibreOffice, Inkscape und Scribus sowie andere Tools wie ImageMagick. [KRO2023]

Die Schwachstelle CVE-2023-36664 betrifft OS-Pipes, die es verschiedenen Anwendungen ermöglichen, Daten auszutauschen, indem Ausgaben einer Anwendung als Eingaben an eine andere weitergeleitet

* 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.

werden. Das Problem ergibt sich aus der Funktion *"gp_file_name_reduce*" in Ghostscript, die mehrere Pfade entgegennimmt und diese kombiniert und vereinfacht, indem relative Pfadverweise aus Effizienzgründen entfernt werden. Wenn jedoch eine speziell erstellte Pfadangabe an die anfällige Funktion übergeben wird, können unerwartete Ergebnisse zurückgegeben werden. Dies kann dazu führen, dass die Validierungsmechanismen überschrieben und Ausnutzungen möglich werden. Darüber hinaus verwendet Ghostscript beim Versuch, eine Datei zu öffnen, eine andere Funktion namens "*gp_validate_path*", um zu überprüfen, ob sich die Datei an einem sicheren Ort befindet. Da die anfällige Funktion jedoch die Speicherortdetails vor der Überprüfung durch diese zweite Funktion ändert, ist es für einen Angreifer einfach, die Sicherheitslücke auszunutzen und Ghostscript dazu zu zwingen, Dateien an Orten zu behandeln, die eigentlich nicht zugelassen sein sollten. [BLEE2023]

Die Schwachstelle betrifft alle Versionen von Ghostscript **vor der Version 10.01.2**, die am 26. Juni veröffentlicht wurde [GHOST2023a]. Da es sich um eine Bibliothek (auch Package genannt) handelt, ist auch **jede Software betroffen, die die Bibliothek einsetzt**, sodass ggf. ein Update bereitgestellt werden muss.

Für Debian wurden die Versionen

- 9.53.3~dfsg-7+deb11u5 (Bullseye) (Debian 11)
- 10.0.0~dfsg-11+deb12u1 (Bookworm) (Debian 12)

veröffentlicht, welche die Schwachstelle schließen [DEB2023].

Bewertung

Ghostscript hat eine hohe Verbreitung und wird sowohl in Linux- als auch in Windows-Umgebungen häufig verwendet. Es ist ein wesentlicher Bestandteil des Common Unix Printing System (CUPS) in Linux, das für Druck- und Druckdienste verwendet wird. Darüber hinaus verwenden viele Anwendungen Ghostscript zum Lesen und Speichern von PDF-Dateien. Daher sind **potenziell viele Systeme** von dieser Schwachstelle **betroffen**.

Angriffsversuche mittels präparierter Dokumente hält das BSI für wahrscheinlich. Um betroffene Systeme abzusichern, ist es daher wichtig, die Betroffenheit zu prüfen und gegebenenfalls auf die neueste Version zu aktualisieren oder Sicherheitspatches anzuwenden.

Die **Ausnutzung** kann allein **durch das Öffnen einer Datei oder automatisierte Verarbeiten** erfolgen, es werden keine weiteren Rechte benötigt. Dies macht es Angreifern einfach, die Schwachstelle mittels Phishing automatisiert auszunutzen. Angreifer könnten auch Dienste attackieren, die einen Upload von Dateien erlauben und diese mit der Bibliothek weiterverarbeiten.

Ein Proof-of-Concept Exploit ist für diese Schwachstelle bereits verfügbar, was bedeutet, dass Angreifer bereits über ein funktionierendes Werkzeug verfügen, um die Schwachstelle auszunutzen.

Es könnte länger dauern, bis jede Software, die von der Ghostscript Bibliothek Gebrauch macht, ein Update zur Behebung der Sicherheitslücke zur Verfügung stellt. Angreifer können die Schwachstelle daher auf absehbare Zeit ausnutzen.

Maßnahmen

Für Linux-Umgebungen

Nutzer von Linux oder Unix sollten über die Paketverwaltung sicherstellen, dass keine Ghostscript-Version vor 10.01.2 installiert ist und ggf. auf die Version 10.01.2 (oder neuer) updaten.

Für Windows-Umgebungen

Nutzer von Windows sollten in den Systemeinstellungen unter "Apps & Features" überprüfen, ob "GPL Ghostscript" installiert ist. Durch einen Klick auf den ggf. vorhandenen Eintrag in der Liste kann die Versionsnummer eingesehen werden. Falls die Versionsnummer kleiner als 10.01.2 ist, so sollte über die offizielle Ghostscript-Downloadseite

[GHOST2023b] der Ghostscript-Installer als "Ghostscript AGPL Release" für die jeweilige Windows-Version heruntergeladen werden. Nach dem Start des Installationsprogramms sollte die Deinstallation der alten Ghostscript-Version bestätigt und die neue Version installiert werden. Unter Umständen müssen bei verändertem Ghostscript-Installationspfad abhängige Programme im Anschluss erneut installiert werden. Es sollte überprüft werden, ob weitere veraltete Versionen von Ghostscript auf dem System vorhanden sind.

Diverse Programme nutzen unter Windows beispielsweise die Ghostscript-Programmdateien mit folgenden Namen:

- gswin32c.exe bzw. gswin64c.exe
- gswin32.exe bzw. gswin64.exe
- gsdll32.dll bzw. gsdll64.dll

Diese Programmdateien können sich bei einer Installation mittels des GPL-Ghostscript-Installers mit Voreinstellungen unter Windows beispielsweise unter einem der folgenden Verzeichnisse befinden:

- C:\Program Files (x86)\gs\gs9.06\bin\
- C:\Program Files\gs\gs9.06\bin\
- C:\gs\gs9.06\bin\

(Die Versionsnummer im Verzeichnisnamen, hier repräsentiert durch "9.06", kann abweichen.)

Für GIMP (ab Version 2, 64-Bit) befinden sich die betroffenen Ghostscript-Bibliotheken unter Windows bei Nutzung des voreingestellten Installationsverzeichnisses beispielsweise unter:

C:\Program Files\GIMP 2\32\bin\libgs-9.dll und C:\Program Files\GIMP 2\bin\libgs-9.dll

(Die Versionsnummer im Dateinamen, hier repräsentiert durch die Zahl 9, kann abweichen; möglich sind mindestens auch: "libgs-10.dll" und "libgs-8.dll".)

Allgemeine Hinweise

Die Liste der in diesem Dokument genannten Anwendungen, die Ghostscript einsetzen, ist nicht abschließend. IT-Sicherheitsverantwortliche sollten daher das in ihrer Organisation genutzte Software-Portfolio individuell auf Hinweise zu dieser Bibliothek prüfen - zum Beispiel über die Webseiten der jeweiligen Hersteller. Sofern diese auf die Notwendigkeit zusätzlicher Updates hinweisen, sollten diese ebenfalls kurzfristig installiert werden.

Bis zum Einspielen einer fehlerbereinigten Version ist zu prüfen, ob die Zugriffsrechte auf die betroffenen Ghostscript-Bibliotheken und -Programmverzeichnisse ohne negative Seiteneffekte entzogen werden können. Zum Einspielen der fehlerbereinigten Version müssen dem updatenden Programm Zugriffsrechte gewährt werden.

Nutzer von Software, die Ghostscript als nicht zentral über einen Paketmanager verwaltete oder nicht eigenständige Version installiert, sollten schnellstmöglich auf eine fehlerbereinigte Version der entsprechenden Software updaten. Dies ist insbesondere unter Windows beispielsweise für Gimp der Fall.

LibreOffice selbst installiert keine Ghostscript-Programmdateien, sondern greift lediglich auf eine eventuell bereits vorhandene Installation zurück [LIB23].

Links

[KRO2023] Proof of Concept Developed for Ghostscript CVE-2023-36664 Code Execution Vulnerability:
https://www.kroll.com/en/insights/publications/cyber/ghostscript-cve-2023-36664-remote-code-execution-vulnerability

[BLEE2023] Critical RCE found in popular Ghostscript open-source PDF library:
https://www.bleepingcomputer.com/news/security/critical-rce-found-in-popular-ghostscript-open-source-pdf-library/

[GHOST2023a]Ghostscript/GhostPDL 10.01.2:
https://github.com/ArtifexSoftware/ghostpdl-downloads/releases/tag/gs10012

[DEB2023] Debian Security Advisory: DSA-5446-1 ghostscript -- security update:
https://www.debian.org/security/2023/dsa-5446

[GHOST2023b] Ghostscript releases:
https://ghostscript.com/releases/

[LIB2023] The Document Foundation Wiki - EPS:
https://wiki.documentfoundation.org/EPS

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.