Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstellen in verschiedenen Microsoft Lösungen

Nr. 2023-205624-1022, Version 1.0, 14.02.2023

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 14. Februar 2023 findet bei Microsoft der turnusmäßige Patchday statt. Wie an jedem zweiten Dienstag eines Monats veröffentlichte der Hersteller heute Sicherheitsupdates für seine Produkte und Informationen zu den Schwachstellen, die mit diesen Aktualisierungen geschlossen werden [MSRC2023].

Dabei fallen von den insgesamt 75 Schwachstellen insgesamt vier Sicherheitslücken besonders ins Gewicht, weil diese nach dem Common Vulnerability Scoring System (CVSS) als "kritisch" bewertet werden. Im Detail handelt es sich um:

- CVE-2023-21716 – eine Schwachstelle in der Dateivorschau für RTF-Dokumente, die in verschiedenen Microsoft Word und SharePoint-Versionen die Ausführung von beliebigem Programmcode ermöglicht. Microsoft bewertet die Sicherheitslücke nach CVSS v3.1 mit einem Score von 9.8 [CVE2023a].
- CVE-2023-21689, CVE-2023-21690 sowie CVE-2023-21692 – drei Schwachstellen, die den Authentifizierungsmechnismus Protected Extensible Authentication Protocol (PEAP) in Microsofts Network Policy Server (NPS) betreffen. Wird ein Windows Server mit Network Policy Server (NPS)-Dienst sowie eine mit PEAP konfigurierte Netzwerkpolicy eingesetzt, besteht grundsätzlich die Gefahr einer Remote Code Execution (RCE). Auch hier wurden die Sicherheitslücken seitens Microsoft nach CVSS v3.1 mit einem Score von 9.8 bewertet [CVE2023b], [CVE2023c], [CVE2023d].

* 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.

BSI-IT-Sicherheitswarnung

Insbesondere im Zusammenhang mit den Schwachstellen in Windows Server schätzt Microsoft Cyber-Angriffe als "eher wahrscheinlich" ein.

Eine aktive Ausnutzung der Sicherheitslücken wurde jedoch noch in keinem der genannten Fälle beobachtet.

Bewertung

Aufgrund der großen Verbreitung von Microsoft Produkten im Allgemeinen stellen diese Lösungen grundsätzlich attraktive Ziele für Cyber-Angriffe dar. IT-Sicherheitsverantwortliche sollten die Veröffentlichungen des Herstellers daher regelmäßig sichten und die Betroffenheit der eigenen Institution prüfen.

Insbesondere die als kritisch bewerteten Sicherheitslücken sollten im aktuellen Patchzyklus jedoch mit besonderer Dringlichkeit behandelt werden. Dabei stellt die Microsoft Office betreffende Schwachstelle CVE-2023-21716 aufgrund der vergleichsweise simplen Ausnutzbarkeit eine erhebliche Bedrohung für IT-Infrastrukturen dar.

Organisationen, die den Network Policy Server (NPS) auf Windows Servern betreiben und eine mit PEAP konfigurierte Netzwerkpolicy einsetzen, sollten auch besonderen Fokus auf die Schwachstellen CVE-2023-21689, CVE-2023-21690 sowie CVE-2023-21692 legen. Nach Microsoft Exploitability Index [MSRC2023e] wird die potenzielle Ausnutzbarkeit dieser Schwachstellen mit Index 1 / "Exploitation more likely" angegeben.

Erfahrungsgemäß suchen Angreifer spätestens nach dem Bekanntwerden von Schwachstellen gezielt nach Exploits und verwundbaren Systemen [ACS2023]. Insofern sollten IT-Sicherheitsverantwortliche kurzfristig Schutzmaßnahmen ergreifen.

Maßnahmen

IT-Sicherheitsverantwortliche sollten die Installation der Patches kurzfristig prüfen. Mit dieser Maßnahme werden nicht nur die kritischen, sondern auch die Schwachstellen mit geringerem Schweregrad geschlossen.

Falls dies aus unterschiedlichen Gründen nicht möglich ist, stellt Microsoft für CVE-2023-21716 einen Workaround zur Verfügung [MSRC2023a], mit dem eine Ausnutzung unterbunden werden kann. Dabei kann Microsofts Office Fileblock Policy genutzt werden, um das Öffnen von RTF-Dateien aus unbekannten Quellen zu blockieren. Bei der Administration sollte jedoch beachtet werden, dass eine unsachgemäße Konfiguration dazu führen kann, dass RTF-Dokumente gar nicht mehr geöffnet werden [MSRC2023b].

Als Mitigation für die Ausnutzung der Schwachstellen CVE-2023-21689, CVE-2023-21690 sowie CVE-2023-21692 gibt Microsoft an, dass der EAP-Typ in der Netzwerkpolicy im NPS so konfiguriert werden kann, dass PEAP kein erlaubter EAP-Typ ist. Microsoft verweist hierfür auf [MSRC2023c] und [MSRC2023d].

Links

[ACS2023] Lebenszyklus einer Schwachstelle:
https://www.allianz-fuer-cybersicherheit.de/SharedDocs/Downloads/Webs/ACS/DE/BSI-CS/BSI-CS_027.pdf?__blob=publicationFile&v=1

[CVE2023a] Microsoft Word Remote Code Execution Vulnerability:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21716

[CVE2023b] Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability (1):
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21689

[CVE2023c] Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability (2):
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21690

[CVE2023d] Microsoft Protected Extensible Authentication Protocol (PEAP) Remote Code Execution Vulnerability (3):
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21692

[MSRC2023] February 2023 Security Updates:
https://msrc.microsoft.com/update-guide/releaseNote/2023-Feb

[MSRC2023a] MS08-026: How to prevent Word from loading RTF files:
https://msrc.microsoft.com/blog/2008/05/ms08-026-how-to-prevent-word-from-loading-rtf-files/

[MSRC2023b] Fehlermeldung in Office, wenn eine Datei durch Registrierungsrichtlinieneinstellungen blockiert ist:
https://support.microsoft.com/kb/922849

[MSRC2023c] Configure a Wireless Connection Profile for PEAP-MS-CHAP v2:
https://learn.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/wireless/e-wireless-access-deployment#bkmk_configureprofile

[MSRC2023d] Configure Network Policies:
https://learn.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-np-configure

[MSRC2023e] Microsoft Exploitability Index:
https://www.microsoft.com/en-us/msrc/exploitability-index

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.