Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Zero-Day Schwachstelle in Microsoft Office

CSW-Nr. 2023-248752-1232, Version 1.2, 09.08.2023

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 hat der Hersteller Microsoft eine Zero-Day-Schwachstelle in der Office-Suite bekanntgegeben, die aktiv ausgenutzt wird. Die Sicherheitslücke wurde nach den Common Vulnerabilities and Exposures unter der Nummer CVE-2023-36884 veröffentlicht und hinsichtlich ihrer Kritikalität mit einem CVSS-Score von 8.3 ("hoch") bewertet (CVSS v3.1).

Nach Angaben des Herstellers kann ein entfernter Angreifer die Ausführung von Code aus der Ferne erreichen, wenn das Opfer dazu gebracht wird, ein speziell präpariertes Microsoft-Office-Dokument zu öffnen.

Weiterhin berichtet Microsoft von einer Phishing-Kampagne, im Rahmen derer die hier beschriebene Schwachstelle bereits ausgenutzt wird. Demnach habe die Bedrohungsakteurgruppe Storm-0978 zuletzt Angriffe auf Verteidigungs- und Regierungsorganisationen in Europa und Nordamerika unternommen. Die dabei genutzten Phishing-Mails mit präparierten Word-Dokumenten wiesen im Betreff einen Bezug zum Ukrainischen Weltkongress auf. Storm-0978, die vor allem für die Verwendung ihrer Backdoor RomCom bekannt ist, ist eine in Russland ansässige Cyberkriminelle-Gruppe, die opportunistische Ransomware- und Erpressungsoperationen sowie gezielte Kampagnen zur Erfassung von Zugangsdaten durchführt, die wahrscheinlich Geheimdienstoperationen unterstützen. Storm-0978 entwickelt und verteilt die RomCom-Backdoor. Der Akteur setzt auch die Ransomware "Underground" ein, die eng mit der im Mai 2022 erstmals im Umlauf befindlichen Ransomware "Industrial Spy" verwandt ist. Die jüngste Kampagne des Akteurs,

* 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.

die im Juni 2023 entdeckt wurde, nutzte die Schwachstelle CVE-2023-36884 aus, um eine Backdoor mit Ähnlichkeiten zu RomCom zu verbreiten [MS2023b].

Eine aktuelle Liste der betroffenen Produktversionen und Hilfestellung sind im Advisory des Herstellers verfügbar [CVE2023a][MS2023a].

Microsoft hat im Rahmen des Juli-Patchday außerdem aktiv ausgenutzte Sicherheitslücken geschlossen, die Angreifer nutzen können, um Sicherheitswarnungen beim Öffnen von Links in Outlook [CVE2023b] oder die Windows-SmartScreen-Warnung [CVE2023c] beim Öffnen von ausführbaren Dateien zu umgehen. Auch ausgenutzte Schwachstellen, die Angreifenden eine Rechteerweiterung ermöglichen, wurden geschlossen ([CVE2023d], [CVE2023e]).

Update 2:
Microsoft stellt mit dem August Patchday ein Update für Microsoft Office bereit [MS2023c]. Das Microsoft Office Defense in Depth Update verhindert die Ausnutzung von CVE-2023-36884. Außerdem wird die Schwachstelle nun als Windows Search Remote Code Execution klassifiziert und nicht mehr als Microsoft Office Schwachstelle.

Bewertung

Textverarbeitungsanwendungen, wie Microsoft Office, sind aufgrund ihrer hohen Verbreitung weltweit ein beliebtes Ziel für Angreifer und werden häufig in Kombination mit Phishing als Einstiegspunkt für Cyber-Angriffe verwendet.

Microsoft berichtet über die Ausnutzung der Schwachstelle durch die russische Angreifer-Gruppe Storm-0978. Die Angriffe von Storm-0978 zielen hauptsächlich auf Verteidigungs- und Regierungsbehörden in Verbindung zur Ukraine ab, um wahrscheinlich Zugangsdaten zu stehlen. Der Akteur stand jedoch auch schon häufig in Verbindung mit Ransomware-Angriffen auf Unternehmen [MS2023b]. Weiterhin muss davon ausgegangen werden, dass – ggf. auch andere Tätergruppen – das öffentliche Bekanntwerden der Sicherheitslücke nutzen, um weitere Exploits zu entwickeln und Angriffsversuche auf Organisationen zu starten, die nicht den oben genannten Verteidigungs- bzw. Regierungssektoren angehören.

Auch wenn die Schwachstelle eine Benutzerinteraktion im Sinne des Öffnens eines präparierten Dokuments erfordert, stuft das BSI den Sachverhalt als schwerwiegend ein. Maßnahmen, um die Schwachstelle zu beheben, sollten schnellstmöglichst getroffen werden, um sicher vor Angriffen auf CVE-2023-36884 zu sein.

Maßnahmen

Für die oben beschriebenen Schwachstelle CVE-2023-36884 [CVE2023a] ist aktuell **kein Patch verfügbar**, es sollten daher die angegebenen Mitigationsmaßnahmen genutzt werden, um die Ausnutzung der Schwachstelle zu verhindern. Außerdem sollten IT-Sicherheitsverantwortliche regelmäßig prüfen, ob ein Patch veröffentlicht wurde.

Folgende Mitigationsmaßnahmen stehen zur Verfügung:

- Allen Microsoft-Office-Anwendungen das Erstellen von Child-Prozessen über die "Attack Surface Reduction (ASR)"-Regeln verbieten **oder**
- unter dem Registry-Schlüssel *HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Internet Explorer\Main \FeatureControl\FEATURE_BLOCK_CROSS_PROTOCOL_FILE_NAVIGATION* neue DWORD-Werte mit den folgenden Namen der Office-Programmdateien anlegen und jeweils auf 1 setzen:
  - Excel.exe
  - Graph.exe
  - MSAccess.exe
  - MSPub.exe
  - Powerpnt.exe
  - Visio.exe
  - WinProj.exe
  - WinWord.exe
  - Wordpad.exe

Update 1:
Aktualisierung der Mitigationsmaßnahmen. DWORD-Wert für PowerPoint muss "Powerpnt.exe" benannt werden.

Microsoft gibt an, dass nach dem Setzen der o.g. Registry-Werte Einschränkungen bei speziellen Nutzungsszenarien auftreten können. Für diesen Fall ist das Risiko der Ausnutzung der Schwachstelle höher zu gewichten als die Einschränkungen. Die Registry-Werte können wieder in den Ausgangszustand gesetzt werden, nachdem der zugehörige Patch veröffentlicht und eingespielt wurde. Eine genauere Erklärung der Mitigationsmaßnahmen sowie weitere Informationen finden sich unter [CVE2023a] und [MS2023b].

Wird das Produkt Microsoft Defender for Office 365 verwendet, verhindert dieses laut Microsoft bereits eine Ausnutzung der Schwachstelle durch präparierte Dokumente. Auch das Produkt Microsoft 365 Apps (ab Version 2302) soll nicht betroffen sein.

Während der Patch zur Schließung von CVE-2023-36884 noch erwartet wird, können mithilfe der Sicherheitsupdates des Juli-Patchdays zumindest die oben beschriebenen Schwachstellen [CVE2023b] bis [CVE2023e] sowie weitere Verwundbarkeiten in Microsoft-Produkten geschlossen werden. Es wird daher dringend empfohlen, diese Updates ebenfalls und unabhängig vom hier beschriebenen Sachverhalt kurzfristig zu prüfen.

Update 2:
IT-Sicherheitsverantwortliche sollten das Microsoft Office Defense in Depth Update [MS2023c] zeitnah installieren, um eine Ausnutzung von CVE-2023-36884 zu verhindern. Vorher getroffene Mitigationsmaßnahmen werden durch das Update nicht mehr benötigt.

Links

[MS2023a] https://msrc.microsoft.com/update-guide/releaseNote/2023-Jul

[MS2023b] https://www.microsoft.com/en-us/security/blog/2023/07/11/storm-0978-attacks-reveal-financial-and-espionage-motives/

[CVE2023a] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36884

[CVE2023b] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-35311

[CVE2023c] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32049

[CVE2023d] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-32046

[CVE2023e] https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-36874

Update 2:
[MS2023c] https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV230003

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.