



SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Kritische Schwachstelle in Microsoft SharePoint Server

CSW-Nr. 2023-240436-1032, Version 1.0, 13.06.2023

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 Abend des 13. Juni 2023 hat Microsoft im Rahmen seines monatlichen Patchdays Updates für zahlreiche Schwachstellen veröffentlicht [MSRC2023] – darunter auch mehrere Patches für Sicherheitslücken, die nach dem Common Vulnerability Scoring System (CVSS) mit Werten von 9.0 und höher als „kritisch“ eingestuft werden.

In den Veröffentlichungen enthalten ist u. a. der Patch für eine „Microsoft SharePoint Server Elevation of Privilege Vulnerability“ (CVE-2023-29357; CVSS-Score 9.8 [CVE2023a]), bei der das Unternehmen darauf hinweist, dass eine Ausnutzung als eher wahrscheinlich einzustufen ist. Ein Angreifer kann mittels manipulierter JWT-Authentifizierungstokens die Authentifizierung umgehen und Benutzerrechte erhalten. Betroffen von der Schwachstelle sind alle Versionen von Microsoft SharePoint Server 2019.

Zu den weiteren Schwachstellen mit einer Bewertung des Schweregrads von „hoch“ oder „kritisch“, die im Juni Patchday von Microsoft geschlossen werden, gehören unter anderem:

- Microsoft Exchange Server Remote Code Execution Vulnerability (CVE-2023-32031; CVSS-Score 8.8 [CVE2023b]):
Die Schwachstelle betrifft Exchange Server 2019 und Exchange Server 2016.

* 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.

- Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability (CVE-2023-29363/32014/32015; CVSS-Score 9.8 [CVE2023c1][CVE2023c2][CVE2023c3]):
Die Schwachstelle betrifft einen Dienst (MSMQ) (TCP-Port 1801), der in Applikationen genutzt werden kann.
- Windows Collaborative Translation Framework Elevation of Privilege Vulnerability (CVE-2023-32009; CVSS-Score 8.8 [CVE2023d]):
Die Schwachstelle könnte im Rahmen einer Attack-Chain ausgenutzt werden.

Darüber hinaus adressiert Microsoft zahlreiche weitere Schwachstellen [MSRC2023].

Bewertung

Aufgrund der weiten Verbreitung von Microsoft-Produkten im Allgemeinen stellen diese Lösungen generell attraktive Ziele für Cyber-Angriffe dar.

Auch wenn der Hersteller zum aktuellen Zeitpunkt von keiner Ausnutzung einer der geschlossenen Schwachstellen berichtet, kann nicht ausgeschlossen werden, dass bereits Angriffe auf deutsche Organisationen in naher Zukunft stattfinden oder stattgefunden haben.

Maßnahmen

IT-Sicherheitsverantwortliche sollten die Installation der veröffentlichten Patches zeitnah prüfen. Dabei sollte die Mitigation der oben beschriebenen „Microsoft SharePoint Server Elevation of Privilege Vulnerability“ (CVE-2023-29357) aufgrund des Schweregrads der Sicherheitslücke mit besonderer Priorität verfolgt werden (siehe [CVE2023a]). Wenn das Update nicht zeitnah eingespielt werden kann, sollte zur Mitigation AMSI kurzfristig für SharePoint aktiviert werden.

Zusätzlich wird dringend empfohlen, auch die weiteren Updates zeitnah zu sichten. Zwar sind hier ebenfalls noch keine Angriffe bekannt, zum Teil geht der Hersteller jedoch davon aus, dass diese mit hoher Wahrscheinlichkeit stattfinden werden.

Links

[MSRC2023] Microsoft June 2023 Security Updates: <https://msrc.microsoft.com/update-guide/releaseNote/2023-Jun>

[CVE2023a] Microsoft SharePoint Server Elevation of Privilege Vulnerability: <https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-29357>

[CVE2023b] Microsoft Exchange Server Remote Code Execution Vulnerability: <https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-32031>

[CVE2023c1] Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability: <https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-29363>

[CVE2023c2] Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability: <https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-32014>

[CVE2023c3] Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability: <https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-32015>

[CVE2023d] Windows Collaborative Translation Framework Elevation of Privilege Vulnerability: <https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-32009>

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-ingestufte Dokumente (außer TLP:CLEAR) dürfen nicht auf Plattformen Dritter (wie Virustotal, Übersetzer, etc.) hochgeladen werden, da die Dokumente dort ggf. Dritten zugänglich gemacht werden.