Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Aktive Ausnutzung einer Schwachstelle in Microsoft Outlook

Hersteller schließt weitere Sicherheitslücken im Rahmen des März-Patchdays

CSW-Nr. 2023-214328-1032, Version 1.01, 16.03.2023

IT-Bedrohungslage*: 2 / Gelb

Sachverhalt

Am Abend des 14. März 2023 hat Microsoft im Rahmen seines monatlichen Patchdays Updates für zahlreiche Schwachstellen veröffentlicht [MSRC2023a] – 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 Outlook Elevation of Privilege Vulnerability“ (CVE-2023-23397; CVSS-Score 9.8 [CVE2023a], bei der das Unternehmen darauf hinweist, dass bereits eine aktive Ausnutzung der Schwachstelle stattfindet. Demnach könnten Angreifende eine manipulierte E-Mail nutzen, um Net-NTLMv2 Hashes abzugreifen. Die Attacke erfolgt bereits **vor dem Öffnen der Mail bzw. vor der Anzeige im Vorschaufenster** – eine Aktion durch den Empfänger ist nicht notwendig. Betroffen sind alle Outlook-Versionen für Windows. Weitere Informationen können dem Blogpost auf der Webseite des Herstellers entnommen werden [MSRC2023b].

Als mit den höchsten CVSS-Scores bewertet, aber nach bisherigem Kenntnisstand noch nicht aktiv ausgenutzt, listet Microsoft folgende Verwundbarkeiten auf:

* 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.

- HTTP Protocol Stack Remote Code Execution Vulnerability (CVE-2023-23392; CVSS-Score 9.8 [CVE2023b]):
  Eine Schwachstelle in vorrangig Windows Server 2022, sofern das HTTP/3-Protokoll aktiviert ist.
- Remote Procedure Call Runtime Remote Code Execution Vulnerability (CVE-2023-21708; CVSS-Score 9.8 [CVE2023c]):
  Betroffen sind Windows Server, deren Port 135 (RPC Endpoint Mapper) erreichbar ist.
- Internet Control Message Protocol (ICMP) Remote Code Execution Vulnerability (CVE-2023-23415; CVSS-Score 9.8 [CVE2023d]):
  Sofern eine Anwendung auf dem System Raw Sockets verwendet, könnte mithilfe manipulierter IP Pakete aus der Ferne Code auf dem System ausgeführt werden.

Darüber hinaus adressiert Microsoft zahlreiche weitere Schwachstellen [MSRC2023a].

***** Fett gedruckt: Angaben zum Ablauf des Angriffs wurden präzisiert - siehe oben. *****

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 insbesondere noch keine detaillierten Angaben dazu macht, wo die beobachtete Ausnutzung der Outlook Schwachstelle zur Rechteausweitung (CVE-2023-23397) stattgefunden hat, kann nicht ausgeschlossen werden, dass bereits Angriffe auf deutsche Organisationen stattfinden/stattgefunden haben.

Maßnahmen

IT-Sicherheitsverantwortliche sollten die Installation der veröffentlichten Patches zeitnah prüfen. Dabei sollte die Mitigation der oben beschriebenen „Microsoft Outlook Elevation of Privilege Vulnerability" (CVE-2023-23397) aufgrund der bereits beobachteten Ausnutzung mit besonderer Priorität verfolgt werden. Zusätzlich wird dringend empfohlen, auch die weiteren Updates kurzfristig zu sichten. Zwar sind hier noch keine Angriffe bekannt, zum Teil geht der Hersteller jedoch davon aus, dass diese mit hoher Wahrscheinlichkeit stattfinden werden.

Laut Microsoft können Angreifende die bei Ausnutzung von CVE-2023-23397 abgegriffenen Net-NTLMv2 Hashes für NTLM-Relay-Angriffe verwenden. NTLM-Relay-Angriffe lassen sich u.a. durch die Aktivierung strikter SMB- und LDAP-Signierung, Extended Protection for Authentication (EPA) oder idealerweise das vollständige Deaktivieren von NTLM-Authentifizierungen mitigieren. Um zu untersuchen, ob bereits ein Angriff auf die eigenen Systeme stattgefunden hat, stellt Microsoft ein Skript zur Verfügung [MSG2023].

Unabhängig vom aktuellen Patchday sollten IT-Sicherheitsverantwortliche außerdem prüfen, ob die Nutzung von NTLM(v2) grundsätzlich noch erforderlich ist oder ein zeitnaher Wechsel zu Kerberos erfolgen kann, das hinsichtlich der Sicherheit einige Vorteile mit sich bringt [LMS2023]. So wird insbesondere die Gefahr von NTLM-Relay Angriffen unterbunden. Weitere Informationen hierzu können dem BSI IT-Grundschutz u.a. in APP.2.2.A9 "Schutz der Authentisierung beim Einsatz von AD DS" [BSI2023] und der Empfehlung von Microsoft entnommen werden [MSD2023].

Links

[BSI2023] APP.2.2 Active Directory Domain Services:
https://bsi.bund.de/dok/1073466

[CVE2023a] Microsoft Outlook Elevation of Privilege Vulnerability:
https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-23397

[CVE2023b] Sicherheitsanfälligkeit im HTTP-Protokollstack bezüglich Remotecodeausführung:
https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-23392

[CVE2023c] Sicherheitsanfälligkeit in der Remoteprozeduraufruf-Runtime bezüglich Remotecodeausführung:
https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-21708

[CVE2023d] Sicherheitsanfälligkeit in Internet Control Message-Protokoll (ICMP) bezüglich Remotecodeausführung:
https://msrc.microsoft.com/update-guide/de-DE/vulnerability/CVE-2023-23415

[LMS2023] NTLM Overview:
https://learn.microsoft.com/en-us/windows-server/security/kerberos/ntlm-overview

[MSD2023] Mitigating Pass-the-Hash (PtH) Attacks and Other Credential Theft, Version 1 and 2:
https://www.microsoft.com/en-us/download/details.aspx?id=36036

[MSFT2009] Credential Relaying Attacks on Integrated Windows Authentication:
https://learn.microsoft.com/en-us/security-updates/securityadvisories/2009/974926

[MSG2023] CVE-2023-23397 script:
https://microsoft.github.io/CSS-Exchange/Security/CVE-2023-23397/

[MSRC2023a] March 2023 Security Updates:
https://msrc.microsoft.com/update-guide/releaseNote/2023-Mar

[MSRC2023b] Microsoft Mitigates Outlook Elevation of Privilege Vulnerability:
https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/

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.