Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Follina-Schwachstelle: Schadcode wird per Microsoft Office eingeschleust

CSW-Nr. 2022-224508-1132, Version 1.1, 15.06.2022

IT-Bedrohungslage*: 3 / Orange

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:WHITE: Unbegrenzte Weitergabe

Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE 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 30.05.2022 veröffentlichte Microsoft Details und Mitigationsmaßnahmen zu einer Schwachstelle in Microsofts Support Diagnostic Tool (MSDT) über das Microsoft Security Response Center (siehe [MIC2022a]). Der Schwachstelle wurde die Common Vulnerabilities and Exposures (CVE)-Nummer CVE-2022-30190 zugewiesen. Nach dem Common Vulnerability Scoring System (CVSS) wird der Schweregrad der Sicherheitslücken auf 7.8 eingestuft (CVSSv3.1) (siehe [MIC2022b]).

Die Schwachstelle kann mithilfe einer präparierten Word-Datei ausgenutzt werden, wodurch Angreifende womöglich in die Lage versetzt werden, auf Basis der im Dokumentenverarbeitungsprogramm enthaltenen Remote Template-Funktion den Download einer HTML-Datei aus dem Internet anzustoßen. Dies kann zur weiteren Ausführung von PowerShell-Code missbraucht werden, wodurch Angreifende Programme installieren, Daten anzeigen, ändern oder löschen könnten.

Erkenntnisse der Sicherheitsforschenden von nao_sec, die bei VirusTotal eine hochgeladene und entsprechend präparierte Word-Datei entdeckt hatten, unterstreichen nun, dass eine aktive Ausnutzung der Schwachstelle stattfindet (siehe [TWI2022]). In der Datei fand sich ebenfalls das Muster 0438, was der

* 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.

Vorwahl des italienischen Ortes Follina entspricht, weshalb die Schwachstelle inzwischen ebenfalls unter diesem Namen diskutiert wird.

Betroffen sind nach bisher gesichteten Medienberichten (siehe [DOUB2022]):

- Office 2013, 2016, 2019, 2021,
- Office Pro Plus und
- Office 365

Bewertung

Aufgrund der großen Verbreitung stellt die Microsoft Office Produktpalette ein attraktives Ziel für Cyber-Angriffe dar. Gleichzeitig erhöhen das Fehlen eines Patches und immer neue Vorgehensweisen beim Social Engineering die Gefahr, Opfer eines Angriffs zu werden.

Wegen der Popularität der Schwachstelle und den bereits veröffentlichten Exploits ist eine kurzfristige, großflächige Ausnutzung der Schwachstelle nicht auszuschließen.

Das Risiko eines Angriffs überwiegt dabei gegenüber dem Risiko, dass durch die Deaktivierung des MSDT-URL-Protokollhandlers Fehlerbehebungen nicht als Links gestartet werden können.

Maßnahmen

Das BSI empfiehlt dringend, bis zur Bereitstellung eines Patches durch den Hersteller die Umsetzung der genannten Workarounds zu prüfen.

Microsoft rät in seinem Blogbeitrag dazu, den MSDT-URL-Protokollhandler zu deaktivieren (siehe [MIC2022a]). Hiermit gehen jedoch auch Beeinträchtigungen der Problemlösungskomponente einher. Die Deaktivierung des MSDT-URL-Protokollhandlers kann in drei Schritten vorgenommen werden:

1. Eingabeaufforderung als Administrator ausführen.
2. Optional: Durch Eingabe von *reg export HKEY_CLASSES_ROOT\ms-msdt <filename>* kann der aktuelle Registry-Key für ein späteres Wiederherstellen der Ursprungskonfiguration in <filename> gespeichert werden.
3. Abschließend durch Eingabe von *reg delete HKEY_CLASSES_ROOT\ms-msdt /f* den entsprechenden Registry-Key löschen.

Fall die Problemlösungskomponente nicht benötigt wird, kann die Konfiguration so bestehen bleiben,
ansonsten kann der gesicherte Registry-Key genutzt werden, um zukünftig nach dem Einspielen des Patches die Ursprungskonfiguration wiederherzustellen.

Update 1:
Microsoft veröffentlichte am 14.06 im Rahmen der monatlichen Updates ein cumulative Update für die Schwachstellen (siehe [MIC2022b], Bereich Revisions). Nach Angaben des Unternehmens schützt der Patch vollumfänglich vor der veröffentlichten Sicherheitslücke. Bei Nutzenden, welche automatische Updates für ihre Systeme eingestellt haben, wird der Patch automatisch installiert.

Da Details zur Schwachstelle bereits seit einigen Tagen bekannt sind, muss jedoch davon ausgegangen werden, dass Systeme, bei denen nicht sofort Schutzmaßnahmen umgesetzt wurden, inzwischen kompromittiert sein könnten. Das System selbst sowie seine Umgebung sollten daher auf Auffälligkeiten und Veränderungen überprüft werden.

Links

[MIC2022a] Guidance for CVE-2022-30190 Microsoft Support Diagnostic Tool Vulnerability

https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability/

[MIC2022b] Microsoft Windows Support Diagnostic Tool (MSDT) Remote Code Execution Vulnerability
https://msrc.microsoft.com/update-guide/en-US/vulnerability/CVE-2022-30190

[TWI2022] Tweet von nao_sec
https://twitter.com/nao_sec/status/1530196847679401984

[DOUB2022] Follina – a Microsoft Office code execution vulnerability
https://doublepulsar.com/follina-a-microsoft-office-code-execution-vulnerability-1a47fce5629e

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 TLP ist ein von der OECD entworfenes Protokoll, welches die Weitergabe von sensitiven Informationen innerhalb eines Informationsverbundes regelt. Die vom Autor adressierten Empfänger dieses Dokumentes haben sich im Vorfeld schriftlich verpflichtet das TLP zu beachten und das Dokument entsprechend den „Ausführungsbestimmungen zum sicheren Informationsaustausch mit TLP“ zu verarbeiten, aufzubewahren, weiterzugeben und zu vernichten.

2) Welche Einstufungen existieren?

   - **TLP:WHITE: Unbegrenzte Weitergabe**
     Abgesehen von urheberrechtlichen Aspekten dürfen Informationen der Stufe TLP:WHITE ohne Einschränkungen frei weitergegeben werden.
   - **TLP:GREEN: Organisationsübergreifende Weitergabe**
     Informationen dieser Stufe dürfen innerhalb der Organisationen und an deren Partner frei weitergegeben werden. Die Informationen dürfen jedoch nicht veröffentlicht werden.
   - **TLP:AMBER: Eingeschränkte interne und organisationsübergreifende Verteilung**
     Informationen dieser Stufe darf der Empfänger innerhalb seiner Organisation auf Basis „Kenntnis nur wenn nötig“ weitergeben. Der Empfänger darf die Informationen zudem an Dritte weitergeben, soweit diese die Informationen zum Schutz des Empfängers oder zur Schadensreduktion beim Empfänger benötigen. Hierfür muss er sicherstellen, dass die „Dritten“ das TLP kennen und die damit verbundenen Regeln einhalten. 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. Meistens werden TLP:RED-Informationen mündlich oder persönlich übergeben.

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:WHITE eingestufte Informationen aus dem Kreis der Verpflichteten.