Bundesamt
für Sicherheit in der
Informationstechnik

Nationales
IT-Lagezentrum BSI

SCHWACHSTELLE | GEFÄHRDUNG | VORFALL | IT-ASSETS

Zeroday-Exploit für Microsoft Betriebssysteme im Umlauf

CSW-Nr. 2021-251937-1132, Version 1.1, 13.09.2021

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: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 7. September 2021 veröffentlichte Microsoft auf seiner Webseite Informationen zu einer bislang nicht gepatchten Sicherheitslücke [MSRC2021], die bereits von Angreifern ausgenutzt wird [TWIT2021]. Hierbei werden präparierte Office-Dokumente versandt. Beim Öffnen dient eine Schwachstelle in der HTML-Rendering-Engine MSHTML von Microsoft dazu, um über den Internet Explorer schadhafte ActiveX-Steuerungselemente nachzuladen und zu installieren. In der Folge ist eine Remote Code Execution (RCE) möglich.

Betroffen sind alle derzeit im Support befindlichen Betriebssysteme – sowohl für Clients als auch für Server. Die Schwachstelle mit der Kennung CVE-2021-40444 hat einen CVSS:3.0-Score von 8.8.

Microsoft weist in seiner Veröffentlichung darauf hin, dass die in Microsoft Office standardmäßig aktivierte geschützte Ansicht die Ge fahr einer Infektion bereits signifikant reduziert. Dennoch können Nutzerinteraktionen dazu führen, dass diese Funktionalität außer Kraft gesetzt wird – beispielsweise dann, wenn das präparierte Office-Dokument außerhalb der geschützten Umgebung geöffnet wird.

Update 1:
Aktuellen Erkenntnissen zufolge schützen die von Microsoft zunächst empfohlenen Workarounds nicht optimal vor der Schwachstelle. Nach dem Öffnen eines präparierten Office-Dokuments sorgen ActiveX-Steuerelemente dafür, dass Schadcode nachgeladen wird. Administratoren wurde daher zunächst geraten, ActiveX für den Internet Explorer zu deaktivieren. Da ein Angriff aber allem Anschein nach auch über

* 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 Dokumentenvorschau des Windows Explorers ausgelöst werden konnte [TWIT2021a], wurde die Warnmeldung entsprechend um einen weiteren Workaround erweitert.

Bewertung

Aufgrund der weiten Verbreitung von Windows Betriebssystemen, dem Fehlen eines Patches und den bereits beobachteten Angriffen geht das BSI von einem hohen Bedrohungspotenzial aus.

Maßnahmen

Zur Mitigation empfiehlt Microsoft die Deaktivierung von ActiveX im Internet Explorer für alle Zonen. Die entsprechende Anpassung der Registry kann [MSRC2021] entnommen werden. Auf vorher installierte ActiveX-Steuerelemente haben die neuen Registry-Einstellungen keinen Einfluss, sodass das Risiko von negativen Randeffekten als sehr gering einzustufen ist.

Die Realisierbarkeit dieser Maßnahme sollte zeitnah geprüft werden. Sobald Microsoft ein Sicherheitsupdate zur Verfügung gestellt hat, sollte dieses ebenfalls kurzfristig installiert werden.

Update 1:
Microsoft zufolge schützt das Öffnen im abgesicherten Modus vor Angriffen, wenn Dokumente direkt aus dem Internet heruntergeladen und geöffnet werden. Weiterhin erkennen und blockieren Sicherheitsforschern zufolge Antiviren-Scanner (wie bspw. Microsoft Defender) den aktuellen Exploit.

Ein dementsprechendes Update wird voraussichtlich zum aktuellen "Patch Tuesday" am 14. 9. 2021 veröffentlicht. Dieses sollte installiert werden sobald dieses zur Verfügung steht.

Links

[MSRC2021] Microsoft MSHTML Remote Code Execution Vulnerability:
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-40444

[TWIT2021] Information der Schwachstellen-Finder auf Twitter:
https://twitter.com/HaifeiLi/status/1435320653503254534

[TWIT2021a] Information bzgl. der Umgehbarkeit der Schwachstelle auf Twitter:
https://twitter.com/GossiTheDog/status/1435570418623070210

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.