Zero-Day-Lücke „Follina“ in MS Office – Hintergründe und Tipps

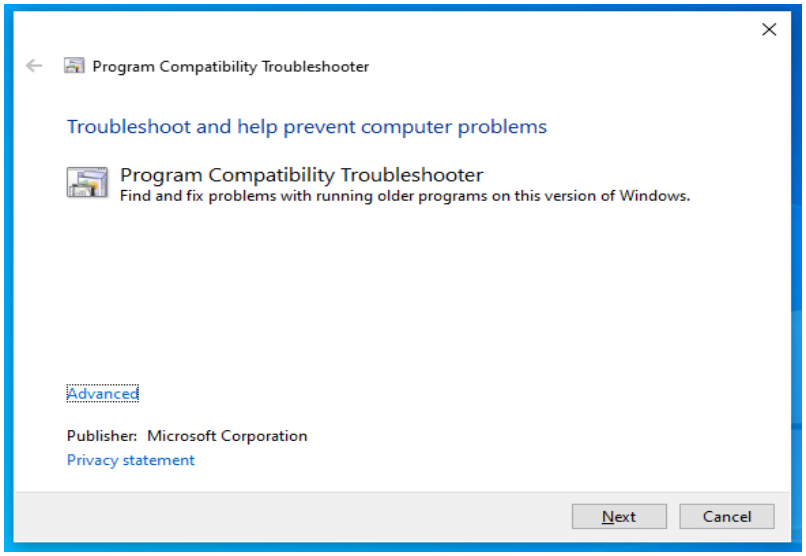
Ein neuer Zero-Day-Bug bei der Remote-Code-Ausführung in Microsoft Office sorgt zurzeit für Wirbel. Genauer gesagt handelt es sich wahrscheinlich um eine Sicherheitslücke bei der Codeausführung, die über Office-Dateien ausgenutzt werden kann.
Sophos beschreibt Lücke und Hintergründe und verweist auf Lösungsmöglichkeiten.

Nach allem, was bislang bekannt ist, gibt es eventuell aber auch andere Möglichkeiten, diese Schwachstelle auszulösen oder zu missbrauchen. Der Sicherheitsforscher Kevin Beaumont hat der Lücke den Namen „Follina“ gegeben, der sich als nützlicher Suchbegriff zu dem Thema erweist, bis eine offizielle CVE-Nummer vergeben ist. Sophos-Experte Paul Ducklin gibt in seinem Blogbeitrag einen Einblick in Hintergründe und Lösungsansätze.

Wie funktioniert die aktuelle Lücke?

- Anwender öffnen eine mit versteckter Malware versehene DOC-Datei, die sie z.B. per E-Mail erhalten haben.
- Das Dokument verweist auf eine normal aussehende https:-URL, die heruntergeladen wird.
- Diese https:-URL verweist auf eine HTML-Datei, die einen JavaScript-Code enthält.
- Das JavaScript wiederum verweist auf eine URL mit der ungewöhnlichen Kennung ms-msdt: anstelle von https:. Unter Windows ist ms-msdt: ein proprietärer URL-Typ, der das MSDT-Software-Toolkit startet. MSDT ist die Abkürzung für Microsoft Support Diagnostic Tool.
- Die zum MSDT via URL übermittelte Befehlszeile führt dazu, dass nicht vertrauenswürdiger Code ausgeführt wird.

Wenn der bösartige ms-msdt:-Link aufgerufen wird, löst er einen MSDT-Befehl mit Befehlszeilenargumenten wie dem folgenden aus: msdt /id pcwdiagnostic .... Wenn es von Hand ausgeführt wird, ohne andere Parameter, lädt dieser Befehl automatisch MSDT und ruft die Programmkompatibilitäts-Fehlerbehebung auf, die harmlos aussieht:



Von hier aus können Nutzer:innen eine App zur Fehlerbehebung auswählen, die verschiedene, support-bezogene Fragen beantwortet, automatisierte Tests in der App

durchführt oder das Problem Microsoft meldet und gleichzeitig verschiedene Daten zur Fehlerbehebung hochlädt. Obwohl Nutzer:innen wahrscheinlich nicht erwarten, nur durch das Öffnen eines Word-Dokuments in dieses Diagnoseprogramm zu kommen, ist die Wahrscheinlichkeit doch erhöht, dass diese Reihe von Popup-Dialogfeldern „akzeptiert“ wird.

Automatische Remote-Skriptausführung
Im „Follina“-Fall sieht es allerdings so aus, als ob die Angreifer auf einige ungewöhnliche, aber auch sehr tückische Optionen gekommen sind, um sich in die Befehlszeile einzuschleichen. In der Folge erledigt die MSDT-Fehlerbehebung ihre Arbeit ferngesteuert. Anstatt gefragt zu werden, wie der Anwendende fortfahren möchte, haben die Cyberkriminellen eine Reihe von Parametern konstruiert, die nicht nur dazu führen, dass die Operation automatisch fortgesetzt wird (zum Beispiel die Optionen /skip und /force), sondern nebenbei auch ein PowerShell-Skript aufrufen. Zu allem Übel muss dieses PowerShell-Skript sich noch nicht einmal in einer Datei auf der Festplatte befinden – es kann in verschlüsselter Quellcodeform direkt aus der Befehlszeile selbst bereitgestellt werden, zusammen mit allen anderen verwendeten Optionen. Im „Follina“-Fall wird die PowerShell laut Hammond dazu verwendet, um eine ausführbare Malware-Datei zu extrahieren und zu starten, die in komprimierter Form bereitgestellt wurde.

Keine Makros erforderlich
Wichtig ist der Fakt, dass dieser Angriff von Word ausgelöst wird, das auf die betrügerische ms-msdt: URL verweist, auf die von einer URL verwiesen wird, die in der DOC-Datei selbst enthalten ist. Aufgrund dieses Vorgehens sind keine VBA-Office-Makros (Visual Basic for Applications) notwendig, sodass dieser Trick auch dann funktioniert, wenn Office-Makros deaktiviert sind.
Deshalb sieht das Ganze wie ein praktisches Office-URL-„Feature“ aus, kombiniert mit einem hilfreichen MSDT-Diagnose-„Feature. In der Tat wird allerdings eine Sicherheitslücke erzeugt, die per Klick einen Remote-Code-Execution-Exploit verursachen kann. Auf diese Weise kann schon das Öffnen eines derart präparierten Word-Dokuments Malware übertragen, ohne dass Nutzer:innen es bemerken.
Tatsächlich schreibt Hammond, dass dieser Trick in einen noch direkteren Angriff umgewandelt werden kann, indem der betrügerische Inhalt in eine RTF-Datei anstatt in eine DOC-Datei verpackt wird. In diesem Fall reiche es aus, nur eine Vorschau des Dokuments im Windows Explorer anzuzeigen, um den Exploit auszulösen, ohne auch nur darauf zu klicken, um es zu öffnen. Allein das Rendern des Thumbnail-Vorschaufensters brächte Windows und Office bereits zum Stolpern.

Was ist zu tun?
Microsoft hat bereits eine offizielle Problemumgehung veröffentlicht und wird hoffentlich zügig einen dauerhaften Patch vorlegen. So praktisch die proprietären ms-xxxx-URLs von Microsoft auch sein mögen, die Tatsache, dass sie darauf ausgelegt sind, Prozesse automatisch zu starten, wenn bestimmte Dateitypen geöffnet oder auch nur in der Vorschau angezeigt werden, ist eindeutig ein Sicherheitsrisiko.

Zudem besteht eine in der Community allgemein anerkannte Problembehandlung darin, einfach die Beziehung zwischen ms-msdt: URLs und dem Dienstprogramm MSDT.EXE zu unterbrechen. Eine detaillierte Beschreibung hierzu gibt Sophos-Experte Paul Ducklin in seinem Blogbeitrag.

Sophos-Produkte unterbinden das Problem
Endpoint-Produkte von Sophos erkennen und blockieren bekannte Angriffe, die über diesen Exploit als Troj/DocDl-AGDX durchgeführt werden. Dieser Erkennungsname kann verwendet werden, um Protokolle sowohl nach DOC-Dateien zu durchsuchen, die den ursprünglichen Download auslösen, als auch nach HTML-Dateien der „zweiten Stufe“, die folgen. E-Mail- und Web-Filter-Produkte von Sophos fangen Angriffsdateien dieser Art wie CXmail/OleDl-AG ab.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.
Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de