SOPHOS
Cybersecurity made simple.

Hacker nutzen Schwachstelle im MS-Formeleditor für Exploits

Eine weitere Anfälligkeit im Formeleditor in Microsoft Office ist nichts Neues. Interessant ist dieses Mal allerdings die Aktivität des angebotenen Patches, Unabhängig von der Lösung des Problems rücken wieder einmal raubkopierte und alte MS-Office-Versionen ins Blickfeld der Cyberkriminellen.

Der Formeleditor (Equation Editor) war sein ganzes Dasein über einer langen Reihe unterschiedlicher Exploits ausgesetzt. Er ist eine Komponente von Microsoft Office, und anstatt ihn noch ein weiteres Mal zu fixen, hat sich der Hersteller dazu entschlossen, einen Patch herauszugeben, der im Wesentlichen den Editor vom System vollständig deinstalliert.

Wann wird ein Exploit wirklich zur Gefahr
Es gibt einen bestimmten Reifepunkt im Lebenszyklus eines Office Exploits, der dann erreicht ist, wenn den Cyberkriminellen Tools zur Nutzung der Schwachstelle in breitem Umfang zur Verfügung stehen. Zuvor trifft der Exploit nur wenige ausgewählte Opfer mit gezielten Angriffen. Ab dem Zeitpunkt jedoch, an dem er weit verbreitet ist, entsteht für eine breite Nutzergruppe eine Bedrohung. Die aktuelle Schwachstelle des Equation Editor erreichte diesen entscheidenden Reifegrad Ende Juni 2019 – genannt CVE-2018-0798.

Charakteristik dieses Exploits
Dieser Exploit wurde während der letzten Monate für gezielte Angriffe eingesetzt und blieb daher meist unter dem Radar. Irgendwann jedoch wurde die Exploit-Implementierung mit nur geringen Änderungen in ein bösartiges Office-Document-Builder-Tool integriert. Erst dies schaffte die Voraussetzungen für eine weitaus breitere Anwendung dieser Angriffstechnik – der nötige Reifegrad war erreicht.
Gemeinsamkeiten des ursprünglichen und jetzt „gereiften“ Exploits sind unverkennbar: So ist beispielsweise der Exploit-Trigger exakt derselbe und der Shellcode (verantwortlich für die Entschlüsselung und Ausführung) ist nahezu identisch mit dem Shellcode, der bei den zuvor gezielten Angriffen verwendet wurde. Obwohl CVE-2018-0798 eine relativ einfache Pufferüberlaufschwachstelle ist, gibt es einige Faktoren, die es schwierig machen, den Exploit-Trigger selbst zu optimieren – daher die praktisch identische Implementierung.
Die Schwachstelle ist hier noch einmal technisch sehr detailliert und anschaulich von den SophosLabs-Experten beschrieben.

Patchen: die einen wollen nicht, die anderen können nicht
Patchen ist also eine gute Möglichkeit, seine Systeme gegen Angriffe abzusichern. Doch einige Anwender haben den Patch nicht installiert, da sie den Formeleditor aus durchaus berechtigen Gründen immer noch für viele Aktionen nutzen. So bleibt er in der Computerumgebung weiter fortbestehen. Und obwohl Microsoft Office mehrfach warnt, das schadhafte Dokument nicht weiterzubearbeiten, umgehen Anwender die Warnmeldungen und infizieren sich selbst. Zudem verbleibt er auch auf zahlreichen Geräten, auf denen raubkopierte und ältere Versionen von Windows und/oder Office laufen. Sie erhalten ja keine Updates.

Wen trifft es am stärksten? Nutzer ohne Erfahrung und wenig Knowhow
Die begehrtesten Exploits fordern vom Nutzer überhaupt keine Aktion ein. Aber im Fall von EqEd erhalten die Hacker einen Zusatznutzen, sofern sie erfolgreich waren: Sie haben es geschafft, Computer von Personen zu infizieren, die eindeutig kein Wissen in punkto Best

Practices zur Computersicherheit besitzen (keine unbekannten Dokumente öffnen, nicht durch zwei unterschiedliche Warnhinweise klicken etc.), und die deshalb auch selten richtig auf Infektionen reagieren.

Diese Schwachstelle ist nicht mit EternalBlue oder BlueKeep vergleichbar, die Tausende von Computern sehr schnell und ohne jegliche Interaktion sowohl der Opfer wie der Angreifer infizieren können. Aber diesen Equation-Editor-Fehler zu verwenden hat einige Vorteile für Hacker: Es zielt auf die die Nutzer, die am wenigsten erfahren und versiert sind – also ein gefundenes Fressen für Cyberattacken.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
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