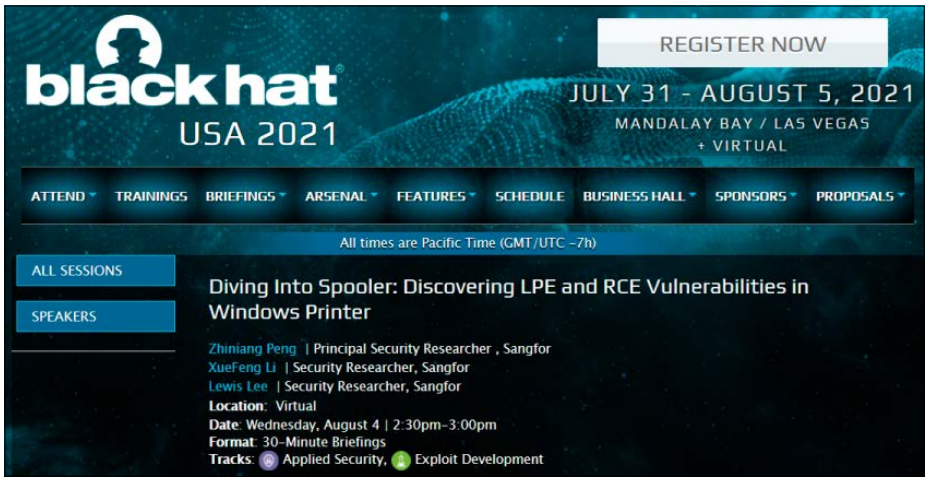

Windows-Lücke mit Druck

PrintNightmare: Zero-Day-Sicherheitslücke in Windows-Druckerwarteschlange

Durch ein fatales Malheur wurde eine kritische Windows-Lücke mehr als einen Monat zu früh publik. Das hat nicht nur Microsoft, sondern insbesondere auch Admins unter Druck gesetzt.

Von Ronald Eikenberg

Wie jedes Jahr tauchten auf der Website der diesjährigen Hackerkonferenz Black Hat im Vorfeld zahlreiche brisante Vorträge im Konferenzplan auf. Darunter eine Session „Diving Into Spooler: Discovering LPE and RCE Vulnerabilities in Windows Printer“ der chinesischen Security-Firma Sangfor. Angekündigt war die Präsentation bislang unbekannter Sicherheitslücken, sogenannte Zero-Day-Lücken, in der Druckerwarteschlange (Spooler) von Windows für den 4. August. Doch für Schlagzeilen sorgten die Forscher viel früher als geplant.

Denn als Microsoft im Rahmen seines Juni-Patchdays ein gefährliches Sicherheitsloch im Windows-Druckerspooler (CVE-2021-1675) stopfte, veröffentlichte einer der Sangfor-Forscher einen auf den Namen PrintNightmare getauften Proof-of-Concept-Exploit (PoC) auf GitHub, der demonstrieren sollte, wie man diese Lücke ausnutzen kann. Es zeigte sich jedoch schnell, dass der Exploit nicht nur gut funktionierte, sondern zu gut. Denn der Angriffscode konnte selbst vollständig gepatchte Windows-Systeme attackieren. Der Sangfor-Forscher hatte versehentlich einen gefährlichen Zero-Day-Exploit in Umlauf gebracht.

Büchse der Pandora

Der Exploit umging den Juni-Patch offenbar. Der Forscher reagierte schnell und löschte seinen Angriffscode bei GitHub. Doch die Büchse der Pandora war längst geöffnet – andere GitHub-Nutzer hatten den Code bereits dupliziert. Inzwischen beherrscht sogar das beliebte Hacking-Tool mimikatz diesen Angriff.

Eilig veröffentlichte Microsoft daraufhin eine erste Warnmeldung. Demnach findet sich der fehlerhafte Code in den Windows-Versionen 7 SP1 bis zum aktuellen Windows 10 21H1. Auch die Server-Betriebssysteme sind betroffen. Besonders besorgniserregend ist, dass die Sicherheitslücke laut Microsoft bereits aktiv von Angreifern ausgenutzt wird.

Remote Code Execution

Laut der Warnmeldung (siehe ct.de/yj6w) handelt es sich um eine Schwachstelle der gefährlichen Kategorie „Remote Code Execution“ (RCE). Angreifer können also aus der Ferne Code auf einem verwundbaren System zur Ausführung bringen. Eine Einschränkung gibt es jedoch: Der Angreifer muss auf dem Zielsystem als Nutzer authentifiziert sein. Dadurch ist PrintNightmare besonders für Unternehmensnetze gefährlich.

Denn Angreifer steigen hier häufig über einen beliebigen Windows-Rechner ein, dessen Nutzer nur eingeschränkte Zugriffsrechte hat. Von dort aus versuchen sie sich weiterzuhangeln. Im schlimmsten Fall gelingt es ihnen so, den kritischen Domaincontroller in ihre Gewalt zu bringen. Damit haben sie das ganze Netzwerk unter ihrer Kontrolle. Wozu das führen kann, zeigt der Fall Emotet.

Bei Einzelplatzrechnern wird es problematisch, wenn der Schadcode aus dem Homeoffice das Intranet des Arbeitgebers über VPN erreichen kann.

Microsoft führt die Schwachstelle inzwischen als CVE-2021-34527. Kurz vor Redaktionsschluss hat das Unternehmen den Notfall-Patch KB5004945 herausgeben, der die Lücke schließen soll (siehe ct.de/yj6w). Den Patch gibt es auch für Windows 7, dessen Support eigentlich seit Januar 2020 abgelaufen ist.

Jetzt patchen!

Windows-Nutzer und -Admins sollten umgehend sicherstellen, dass der Patch installiert ist. Als dieser Artikel entstand, musste das Update noch von Hand installiert werden. Man kann jedoch davon ausgehen, dass Microsoft den Security-Fix zeitnah auch über Windows Update verteilt. Forscher warnen, dass es trotz Patch möglich sein könnte, die Lücke auszunutzen, wenn die Windowsfunktion „Point and Print“ zu freizügig eingestellt ist („NoWarningNoElevationOnInstall“). Admins sollten die Einstellung daher sicherheitshalber checken. *(rei@ct.de)* c't

Aktuelle Informationen: ct.de/yj6w