Microsoft Remote Desktop Services (RDP) Schwachstelle «BlueKeep» in Windows für Fernwartungsfunktion betroffen

Der Grund dafür ist eine als "kritisch" eingestufte Sicherheitslücke (CVE-2019-0708) in der Fernwartungsfunktion Remote Desktop Services (RDP). Diese kritische Schwachstelle kann zu ähnlich verheerenden Angriffen führen, wie wir sie 2017 mit WannaCry erleben mussten.

Um was geht es?

Microsoft und das Bundesamt für Sicherheit in der Informationstechnik (BSI) haben in einer Pressemitteilung vor einer Schwachstelle im Remote-Desktop-Protocol-Dienst (Remote Desktop Services) einiger Windows-Versionen gewarnt, welche als «kritisch» eingestuft wurde.

Wenn der Remote Desktop Services aktiviert ist, kann ein Angreifer die Lücke aus der Ferne und ohne Authentifizierung ausnutzen. Dafür muss er lediglich eine präparierte RDP-Anfrage (mit Schadcode) an einen verwundbaren Computer senden und diesen auf dem infizierten Computer ausführen. Für eine erfolgreiche Attacke ist ein Mitwirken des Opfers nicht notwendig. Funktioniert alles, kann sich die Malware vom verseuchten Computer wurmartig weiterverbreiten und ganze Netzwerke anstecken.

Microsoft und BSI raten den Nutzern den Patch umgehend einzuspielen, da die Schwachstelle einen Angriff mit Schadsoftware ermöglicht, welche sich schnell und selbstständig weiterverbreitet.

Betroffene Windows Versionen:
Windows XP*, Windows 7, Windows 2003 Windows Server 2008 R2, und Windows Server 2008 (Microsoft bietet noch Support).
*(kein Support mehr durch Microsoft, jedoch macht Microsoft bei dieser Schwachstelle eine Ausnahme und liefert trotz abgelaufenem Support noch Sicherheitspatches für Windows XP).

Nicht betroffen Windows Versionen:
Windows 8, Windows 8.1, Windows 10, Windows Server 2012 und Windows Server 2012 R2, Windows Server 2016, Windows Server 2019

Wie ist die Bedrohungslage auf meiner Anlage?

Bislang haben weder BSI noch Microsoft einen Fall beobachtet, in dem die Lücke tatsächlich aktiv ausgenutzt wurde. Allerdings sind sich beide einig, dass sich dies sehr wahrscheinlich bald ändern wird.

Die Ransomware WannCry legte ab Mai 2017 weltweit hunderttausende Windows-Systeme lahm und befiel auch die Infrastruktur grosser Unternehmen und Behörden. Sie verbreitete sich unter anderem, indem sie sich unter Ausnutzung bekannter Sicherheitslücken wie ein klassischer Computerwurm von einem Rechner im Netzwerk zum nächsten "durchfrass".
Nutzer potenziell verwundbarer Systeme sollten diese umgehend aktualisieren. Wer Windows-Versionen verwendet, die Microsoft nicht mehr unterstützt (beispielsweise XP oder Server 2003), muss die Updates gegebenenfalls manuell herunterladen.

Diese Microsofts Links enthalten die Downloads für die betroffenen Betriebssysteme:

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
(Windows 7, Windows Server 2008 R2, und Windows Server 2008)

https://support.microsoft.com/help/4500705
(Windows 2003 und XP)

Wie kann ich mich dagegen schützen?

Wer betroffene Windows-Versionen einsetzt, sollte aufgrund von möglichen Angriffen so schnell wie möglich die aktuellen Sicherheitsupdates (über Windows Update angebotenen) installieren. Zudem sollte man die RDP-Funktion wirklich nur nutzen, wenn es nicht anders geht. Ansonsten deaktiviert man sie besser. Dies, weil für die Sicherheitslücke bereits ein PoC (Proof of Concept - eine detaillierte Erklärung der Lücke) besteht. Somit ist es nur eine Frage der Zeit, bis der erste Wurm auftaucht, der sich durch die Lücke automatisiert verbreitet.

Das BSI rät zur Deaktivierung der Remote Desktop Services, falls diese nicht genutzt würden oder das Blockieren von TCP/UDP-Port 3389 und dem Aktivieren der Network Level Authentication (NLA).

Beim Nutzen von Remote Desktop Services sollten Verbindungen von aussen auf bestimmte Netzbereiche oder Adressen beschränkt und Remote-Desktop-Protocol-(RDP)-Anmeldungen zu Kontrollzwecken protokolliert werden.

Empfehlung
Update Service Modul
Mit dem Update-Service übernimmt Rittmeyer das Testen und installieren der Patches und Hotfix von Microsoft und RITOP. Besonders für das Betriebssystem wird empfohlen, in regelmässigen Abständen alle verfügbaren Sicherheitsupdates zu installieren, um bekannte Sicherheitslücken zu schliessen.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity