الجمهورية العربية السورية
الهيئة الوطنية لخدمات الشبكة
مركز أمن المعلومات

National Agency for Network Services
Information Security Center

تحذير أمني عن ثغرة جديدة في أنظمة التشغيل Windows

ثغرة جديدة بمستوى خطورة عالي بحسب الجهات المتخصصة بتصنيف الثغرات، تعتبر ثغرة BlueKeep من فئة ثغرات RCE: Remote Code Execution، وهي تستهدف خدمات الاتصال البعيد Remote Desktop Services، بحيث أنه لا ضرورة بالمهاجم أن يعرف أي بيانات دخول لاستغلال هذه الثغرة، وقد تم التحذير بخطورة هذه الثغرة وإمكانية تسببها بالسيطرة على عدد كبير من الحواسب في زمن قصير نسبياً مع التأكيد على ضرورة إغلاقها وبشكل فوري، وقد تم تصنيف هذه الثغرة بالرمز: CVE-2019-0708

التأثير Impact

قد يتمكن المهاجمون بعد نجاحهم في استغلال هذه الثغرة من تنفيذ رمازات تعسفية ضمن الأنظمة المستهدَفة، بالإضافة إلى تحميل وتنصيب برمجيات خبيثة تستهدف تتبع نشاط المستخدمين، والسماح للمهاجمين بالاطلاع على البيانات الموجودة ضمن الأنظمة المستهدَفة وتغييرها وحتى حذفها، وقد يتمكن المهاجمون أيضاً من إنشاء حسابات لمستخدمين جدد على الأنظمة المستهدَفة وبسماحيات عالية.

الاستغلال Exploitation

يتم استغلال هذه الثغرة من خلال محاولة المهاجمين الاتصال بنظام التشغيل المستهدَف –بالطبع المهاجم لا يملك حساباً أو أي بيانات دخول– مستخدماً لهذا الاتصال البرتوكول RDP: Remote Desktop Protocol، وعلى المهاجمين لإتمام عملية الاستغلال ارسال طلبات خاصة سبق وقد أُعدت خصيصاً لهذه الغاية.

الإصدارات المتأثرة Affected Products and Versions

Windows XP
Windows Server 2003
Windows Vista
Windows 7
Windows Server 2008
Windows Server 2008 R2

الحلول Solutions

نظراً لخطورة هذه الثغرة من حيث التأثير وإمكانية الاستغلال، فإن الشركة المطورة لأنظمة التشغيل Windows توصي وبشدة بتطبيق التحديثات على الإصدارات المتأثرة لإغلاق هذه الثغرة وبشكل فوري:

https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

سلمان علي
سليمان

Digitally signed by سليمان علي سليمان
DN: c=SY, ou=مركز أمن المعلومات, o=National Agency for Network Services (NANS), 0.9.2342.19200300.100.1.1=10170009529, cn=سلمان علي سليمان
Date: 2019.06.09 11:47:47 +03'00'