BOLETÍN DE ALERTA

Boletín Nro.: 2019-03
Fecha de publicación: 16/08/2019
Tema: Vulnerabilidades críticas del servicio de escritorio remoto de Microsoft Windows

- CVE-2019-1181
- CVE-2019-1182
- CVE-2019-1222
- CVE-2019-1226

Sistemas afectados:

El equipo de seguridad de Microsoft alerta de cuatro vulnerabilidades CVE-2019-1181 y CVE-2019-1182 que afectan a todas las versiones de Windows 10, además de las versiones server 2019, Windows 7 SP1, Windows Server 2008 R2 SP1, Windows Server 2012, Windows 8.1 y Windows Server 2012 R2.

En el caso de las vulnerabilidades CVE-2019-1222 y CVE-2019-1226 afectan solamente a las ediciones de Windows 10 y Windows Server.

Descripción:

Las vulnerabilidades pueden ser ser explotadas por atacantes remotos no autenticados para tomar el control de un afectado sistema **sin requerir ninguna interacción del usuario.**

Dos de las vulnerabilidades críticas que pueden ser explotadas remotamente y presentan características similares a BlueKeep; como es el hecho de que podrían permitir que un malware se propague automáticamente hacia otros equipos vulnerables sin necesidad de interacción por parte de la víctima (características de gusano).

Para explotar los dos primeros fallos, que permiten ejecutar código de manera arbitraria, un atacante no autenticado solo necesitará enviar una solicitud especialmente diseñada al sistema elegido como blanco a través de RDP.

Los sistemas afectados que no hayan instalado el último parche seguirán siendo vulnerables a la explotación mediante RCE si un atacante obtiene las credenciales que le permitan autenticarse

Impacto:

Un atacante que explote exitosamente esta vulnerabilidad podrá ejecutar código en el equipo comprometido e instalar programas, ver y/o modificar información e incluso crear nuevas cuentas con altos niveles de permisos.

Solución:

Microsoft ha lanzado parches que corrigen las vulnerabilidades. Se recomienda instalar lo antes posible las últimas actualizaciones sobre Remote Desktop Protocol (RDP).

Prevención:

Microsoft recordó a los usuarios que Windows 7 y Windows Server 2008 R2 no tendrán soporte extendido y no recibirán actualizaciones a partir del 14 de enero de 2020. Se recomienda actualizar.

Se recomienda también mantener actualizados los sistemas y software a la última versión disponible para evitar ataques como los expuestos en el presente documento.

Información adicional:
https://portal.msrc.microsoft.com/en-us/security-guidance/releasenotedetail/312890cc-3673-e911-a991-000d3a33a34d

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1181

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1182

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1222

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1226