BOLETÍN DE ALERTA

Boletín Nro.: 2019-02
Fecha de publicación: 16/05/2019
Tema: Vulnerabilidad crítica CVE-2019-0708 del servicio de escritorio remoto de Microsoft Windows

Sistemas afectados:

- Windows 7 for 32-bit Systems Service Pack 1
- Windows 7 for x64-based Systems Service Pack 1
- Windows Server 2008 for 32-bit Systems Service Pack 2
- Windows Server 2008 for Itanium-Based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2
- Windows Server 2008 for x64-based Systems Service Pack 2 (Server Core installation)
- Windows Server 2008 R2 for Itanium-Based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1
- Windows Server 2008 R2 for x64-based Systems Service Pack 1 (Server Core installation)
- Windows XP SP3 x86
- Windows XP Professional x64 Edition SP2
- Windows XP Embedded SP3 x86
- Windows Server 2003 SP2 x86
- Windows Server 2003 x64 Edition SP2

Descripción:

Se ha descubierto una nueva vulnerabilidad, identificada como CVE-2019-0708, que permite la ejecución remota de código, en servicios de escritorio remoto (RDP), que afecta a algunas versiones de Windows, citadas más arriba.

Un atacante que explote exitosamente esta vulnerabilidad podría ejecutar código arbitrariamente en el sistema destino, instalar programas, ver, cambiar o eliminar datos, o crear nuevas cuentas.

Dado el impacto potencial de la vulnerabilidad, Microsoft tomó la decisión de hacer que las actualizaciones (parches) estén disponibles también para las plataformas que ya no cuentan con el soporte general como Windows XP y Windows server 2003.

Las versiones de Windows 8 y Windows 10 no se ven afectados por esta vulnerabilidad.

Aún no se cuenta con reportes del impacto de dicha vulnerabilidad, pero es posible que sea explotada en forma masiva en un futuro cercano.

Impacto:

Un atacante que explote exitosamente esta vulnerabilidad podría ejecutar código arbitrariamente en el sistema destino, pudiendo ganar el control completo del mismo.

Solución:

Microsoft ha lanzado un parche que corrige la vulnerabilidad. Se recomienda instalar las actualizaciones tan pronto como sea posible, inclusive si se plantea deshabilitar los servicios de escritorio remoto.

Prevención:

- Deshabilitar el servicio de escritorio remoto si no son necesarios. Si ya no es necesario este servicio en el sistema, se debe considerar deshabilitarlo como una mejor práctica de seguridad. La desactivación de servicios no utilizados e innecesarios ayuda a reducir su exposición a las vulnerabilidades de seguridad.
- Habilitar la autenticación de red (NLA), para evitar que los atacantes no autenticados exploten la vulnerabilidad. Con el NLA activado, los atacantes primero tendrían que autenticarse para el servicio de escritorio remoto, usando una cuenta válida en el sistema destino antes de que el mismo pueda explotar la vulnerabilidad.
- Bloquear el puerto 3389 en el firewall perimetral de la organización. El puerto 3389 se usa para iniciar la conexión con el componente afectado. Bloqueando este puerto en el firewall perimetral ayudará a proteger los sistemas que están detrás de ese servidor de seguridad.

Información adicional:
https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/vulnerabilidad-critica-del-servicio-de-escritorio-remoto-de-windows

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708