COMUNICADO SOBRE VULNERABILIDAD QUE AFECTA A DIVERSAS VERSIONES DE WINDOWS (CVE-2019-0708)

Fecha de lanzamiento Original: 14 de Mayo de 2019 | Última revisión 15 de Mayo de 2019

En relación al parche de seguridad que Microsoft ha liberado para los sistemas operativos Windows XP, Windows 7, Windows 2003 y Windows Server 2008 R2, y dada la amplitud de su uso entre la comunidad, el CSIRT de Gobierno hace un llamado a los usuarios para que actualicen las versiones de seguridad de este sistema e instalen los parches, migren las plataformas (sin soporte como XP) a aquellas que tengan soporte, y bloqueen el acceso al puerto 3389 si es que llegase a estar expuesto a internet.

De acuerdo a lo informado por la Compañía, existe una vulnerabilidad de ejecución remota de código en Servicios de Escritorio Remoto, conocido como Servicios de Terminal Server, la que se puede explotar cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía solicitudes especialmente diseñadas. Esta vulnerabilidad es previa a la autenticación y no requiere la interacción del usuario.

Un atacante que aproveche esta vulnerabilidad podría ejecutar un código arbitrario en el sistema de destino y entonces instalar programas; ver, cambiar, o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario.

La actualización repara la vulnerabilidad al corregir la forma en que los Servicios de Escritorio Remoto manejas las solicitudes de conexión.

Los parches para actualizar los sistemas operativos están a disposición en el enlace oficial de Microsoft, al cual se puede acceder directamente en:

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

Contactos

https://www.csirt.gob.cl

+(562) 24863850

https://www. linkedin.com/company/csirt-gob

@CSIRTGOB