Alerta de Seguridad Informática

CSIRT
Equipo de Respuesta ante Incidentes de Seguridad Informática

Alerta de seguridad informática	9VSA-00033-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	13 de agosto de 2019
Última revisión	13 de agosto de 2019

NOTIFICACIÓN
La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes, del propio fabricante e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información entregada por Microsoft este martes 13 de agosto, referente a actualizaciones de seguridad para hacer frente a vulnerabilidades calificadas como críticas y que pueden permitir el control remoto de un atacante sin requerir información.

Vulnerabilidad

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

Impacto

Existe una vulnerabilidad de ejecución remota de código en los Servicios de Escritorio Remoto (anteriormente conocidos como Servicios de Terminal Server) cuando un atacante no autenticado se conecta al sistema de destino mediante RDP y envía solicitudes especialmente diseñadas.
Esta vulnerabilidad es pre-autenticación y no requiere interacción del usuario. Un atacante que explotara con éxito esta vulnerabilidad podría ejecutar código arbitrario en el sistema de destino. Un atacante podría instalar programas; ver, cambiar o eliminar datos; o crear nuevas cuentas con plenos derechos de usuario.

Productos Afectados

- Windows 10, versiones 32-bit y x64.
- Windows 7, versiones 32-bit y x64, service pack 1.
- Windows 8.1, versiones 32-bit y x64.
- Windows RT 8.1
- 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 Server 2012
- Windows Server 2012 (Server Core installation)
- Windows Server 2012 R2
- Windows Server 2012 R2 (Server Core installation)
- Windows Server 2016
- Windows Server 2016 (Server Core installation)
- Windows Server 2019
- Windows Server 2019 (Server Core installation)
- Windows Server, version 1803 (Server Core Installation)
- Windows Server, version 1903 (Server Core installation)

Mitigación

Aplicar las actualizaciones publicadas por el fabricante.
Deshabilitar el servicio RDP si no es utilizado.

Enlace

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

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno
de Chile
Fecha: 2019.08.13
22:30:04 -04'00'