Alerta de seguridad informática	9VSA-00046-001
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	09 de agosto de 2019
Última revisión	09 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 referente a vulnerabilidades detectadas que pueden comprometer la seguridad en sus sistemas operativos. Si bien los CVE's ya fueron advertidos a la comunidad en informes pasados[1], debido al hallazgo de un nuevo exploit llamado **DejaBlue,** y por su parecido con **BlueKeep** (otra falla de seguridad de RDP expuesta en mayo), el CSIRT de Gobierno ha estimado necesario publicar esta alerta de seguridad.

Vulnerabilidad

CVE-2019-1181
CVE-2019-1182

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 la autenticación previa y no requiere la 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.

Para aprovechar esta vulnerabilidad, un atacante debería enviar una solicitud especialmente diseñada al Servicio de escritorio remoto de los sistemas de destino a través de RDP.

[1] 9VSA-00033-001 en: https://www.csirt.gob.cl/media/2019/08/9VSA-00033-001.pdf y 9VSA-00034-001 en: https://www.csirt.gob.cl/media/2019/08/9VSA-00034-001.pdf, ambos publicados el 13 de agosto de 2019

Vulnerabilidad

CVE-2019-1223

Impacto

Existe una vulnerabilidad de denegación de servicio en el Protocolo de escritorio remoto (RDP) cuando un atacante se conecta al sistema de destino mediante RDP y envía solicitudes especialmente diseñadas. Un atacante que aprovechara esta vulnerabilidad con éxito podría hacer que el servicio RDP en el sistema de destino dejara de responder.

Para aprovechar esta vulnerabilidad, un atacante necesitaría ejecutar una aplicación especialmente diseñada contra un servidor que proporciona servicios de Protocolo de escritorio remoto (RDP).

Vulnerabilidad

CVE-2019-1224
CVE-2019-1225

Impacto

Existe una vulnerabilidad de divulgación de información cuando el servidor RDP de Windows revela incorrectamente el contenido de su memoria. Un atacante que explotara con éxito esta vulnerabilidad podría obtener información para comprometer aún más el sistema.

Para aprovechar esta vulnerabilidad, un atacante tendría que conectarse de forma remota a un sistema afectado y ejecutar una aplicación especialmente diseñada.

Productos Afectados

Windows 10 for 32-bit Systems
Windows 10 for x64-based Systems
Windows 10 Version 1607 for 32-bit Systems
Windows 10 Version 1607 for x64-based Systems
Windows 10 Version 1703 for 32-bit Systems
Windows 10 Version 1703 for x64-based Systems
Windows 10 Version 1709 for 32-bit Systems
Windows 10 Version 1709 for 64-based Systems
Windows 10 Version 1709 for ARM64-based Systems
Windows 10 Version 1803 for 32-bit Systems
Windows 10 Version 1803 for ARM64-based Systems
Windows 10 Version 1803 for x64-based Systems
Windows 10 Version 1809 for 32-bit Systems
Windows 10 Version 1809 for ARM64-based Systems
Windows 10 Version 1809 for x64-based Systems
Windows 10 Version 1903 for 32-bit Systems
Windows 10 Version 1903 for ARM64-based Systems
Windows 10 Version 1903 for x64-based Systems
Windows 7 for 32-bit Systems Service Pack 1
Windows 7 for x64-based Systems Service Pack 1
Windows 8.1 for 32-bit systems
Windows 8.1 for x64-based systems
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

Se hace especial hincapié en aplicar las actualizaciones liberadas por Microsoft, además de lo anterior se recomiendan los siguientes puntos de revisión:

- Deshabilitar el servicio RDP si no es requerido.
- Habilite la autenticación de nivel de red (NLA) en sistemas que ejecutan ediciones compatibles de Windows 7, Windows Server 2008 y Windows Server 2008 R2
- Verificar que el puerto TCP 3389 en el firewall perimetral se encuentre denegado.
- Monitorear el uso del puerto TCP 3389 en su red.
- Para cualquier servicio de administración remota, se recomienda utilizar VPN, para no exponer puertos o aplicaciones de administración

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-2019-1223
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1224
https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1225

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.09 18:19:50 -03'00'