Alerta de seguridad informática	9VSA-00008-002
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	17 de junio de 2019
Última revisión	07 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.

El lanzamiento original de esta alerta se hizo con el título "Alerta (AA19-168A)". Su publicación se hizo en el sitio web del CSIRT y a través de redes sociales. El reporte fue obtenido desde CISA, Departamento de Homeland Security del Gobierno de los Estados Unidos de América. La información fue publicada originalmente en: https://www.us-cert.gov/ncas/alerts/AA19-168A

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la siguiente alerta de vulnerabilidad advertida por el Departamento de Seguridad Interior de los Estados Unidos a través del sitio web oficial de la Agencia de Ciberseguridad y de Seguridad de las Infraestructuras, conocida por sus siglas en inglés como CISA, la que emitió esta Alerta para proporcionar información sobre la vulnerabilidad conocida como "BlueKeep", que existe en Sistemas Operativos de Microsoft Windows (OS), incluidas las versiones de 32 y 64 bits, así como todas las versiones del Service Pack. Un atacante puede aprovechar esta vulnerabilidad para tomar el control de un sistema afectado.

Vulnerabilidad

CVE-2019-0708

Impacto

BlueKeep (CVE-2019-0708) existe dentro del Protocolo de Escritorio Remoto (RDP, por sus siglas en inglés) utilizado por los sistemas operativos Microsoft Windows enlistados anteriormente. Un atacante puede aprovechar esta vulnerabilidad para realizar la ejecución remota de código en un sistema desprotegido.

De acuerdo a Microsoft, un atacante puede enviar paquetes especialmente diseñados a uno de estos sistemas operativos que tienen el RDP habilitado. **[1]** Después de enviar con éxito los paquetes, el atacante podría realizar una serie de acciones: agregar cuentas con todos los derechos de usuario; visualización, modificación o eliminación de datos; o instalando programas. Esta explotación, que no requiere la interacción del usuario, debe ocurrir antes de que la autenticación sea exitosa.

BlueKeep se considera "manipulable" porque el malware que explota ésta vulnerabilidad en un sistema, podría propagarse a otros sistemas vulnerables. Por lo tanto, una explotación de BlueKeep sería capaz de propagarse rápidamente de manera similar a los ataques de malware de WannaCry de 2017. **[2]**

CISA, en coordinación con partes interesadas externas y ha determinado que Windows 2000 es vulnerable a BlueKeep.

Productos Afectados

BlueKeep existe en los siguientes Sistemas Operativos de Microsoft Windows (OS), incluidas las versiones de 32 y 64 bits, así como todas las versiones del Service Pack:

- Windows 2000
- Windows Vista
- Windows XP
- Windows 7
- Windows Server 2003
- Windows Server 2003 R2
- Windows Server 2008
- Windows Server 2008 R2

Un atacante puede aprovechar esta vulnerabilidad para tomar el control de un sistema afectado.

Mitigación

Se hace un llamado a los usuarios y administradores a que revisen el Aviso de seguridad de Microsoft **[3]** y la Guía del cliente de Microsoft para el CVE-2019-0708 **[4]** y apliquen las medidas de mitigación adecuadas lo antes posible:

Instale los parches disponibles. Microsoft ha lanzado actualizaciones de seguridad para parchar esta vulnerabilidad. Microsoft también ha lanzado parches para una serie de sistemas operativos que ya no son oficialmente compatibles, incluidos Windows Vista, Windows XP y Windows Server 2003. CISA alienta a los usuarios y administradores a probar los parches antes de la instalación.

Para los sistemas operativos que no tienen parches o sistemas que no pueden ser parcheados, se pueden usar otros pasos de mitigación para ayudar a protegerse frente a BlueKeep:

- **Actualizar los sistemas operativos al final de su vida útil** (EOL). Considere la posibilidad de actualizar cualquier sistema operativo EOL que no sea compatible con Microsoft a un sistema operativo más nuevo y compatible, como Windows 10.

- **Deshabilitar servicios innecesarios.** Deshabilita los servicios que no están siendo utilizados por el sistema operativo. Esta práctica limita la exposición a vulnerabilidades.

- **Habilitar la autenticación de nivel de red.** Habilite la autenticación de nivel de red en Windows 7, Windows Server 2008 y Windows Server 2008 R2. Hacerlo obliga a que una solicitud de sesión se autentique y la mitigación pueda ser efectiva ante BlueKeep, ya que para aprovechar la vulnerabilidad se requiere una sesión no autenticada

- **Bloquee el puerto 3389 del Protocolo de control de transmisión (TCP) en el firewall perimetral de la empresa.** Debido a que el puerto 3389 se utiliza para iniciar una sesión RDP, el bloqueo impide que los atacantes exploten BlueKeep desde fuera de la red del usuario. Sin embargo, esto bloqueará las sesiones RDP legítimas y es posible que no impida que se inicien sesiones no autenticadas dentro de una red.

Enlace

[1] Advertencia de Seguridad de Microsoft para CVE-2019-0708 disponible en: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
[2] Reporte de Prensa de la Casa Blanca que atribuye el ataque WannaCry Malware a Corea del Norte disponible en: https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/
[3] Advertencia de Seguridad de Microsoft para CVE-2019-0708 disponible en: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708
[4] Guía de Usuario de Microsoft para CVE-2019-0708 disponible en: https://support.microsoft.com/en-us/help/4500705/customer-guidance-for-cve-2019-0708

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.09.07 19:47:53 -04'00'