Alerta de Seguridad Informática (9VSA-00020-001)

Nivel de Riesgo: Alto

Tipo: Vulnerabilidad

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio 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 comparte una información publicada por Microsoft referente a una vulnerabilidad existente en Windows Defender Application Control (WDAC)

Vulnerabilidad

CVE-2019-1167

Impacto

Esta vulnerabilidad podría permitir a un atacante omitir la característica de seguridad en Windows Defender Application Control aprovechando de eludir el modo de lenguaje restringido en PowerShell Core.

Para aprovechar la vulnerabilidad, un atacante primero deberá tener acceso de administrador a la máquina local donde PowerShell se está ejecutando en el modo de lenguaje restringido. Al hacer eso, un atacante podría aprovechar la depuración de scripts para abusar de los módulos firmados de una manera no intencionada.

Productos afectados

PowerShell Core Version 6.1 y 6.2

Mitigación

Actualizar la versión de PowerShell comprometida a 6.1.5 y 6.2.2 según corresponda, ya que la actualización corrige como funciona PowerShell en el modo de lenguaje restringido.

Enlaces

https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2019-1167

https://github.com/PowerShell/PowerShell/security/advisories/GHSA-5frh-8cmj-gc59

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT
Gobierno de
Chile

Firmado digitalmente
por CSIRT Gobierno de
Chile
Fecha: 2019.07.17
18:53:27 -04'00'