Alerta de seguridad cibernética	9VSA20-00300-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	15 de septiembre de 2020
Última revisión	15 de septiembre de 2020

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 obtenida de Microsoft referente una vulnerabilidad crítica que permite la elevación de privilegios en controladores de dominio de Active Directory. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2020-1472

CVE-2020-1472

La vulnerabilidad crítica permitiría a un atacante cambiar y restablecer las credenciales de un controlador de dominio de Active Directory, la única condición es la capacidad de establecer una conexión TCP con el DC vulnerable, no es necesario tener credenciales de dominio.
Esta vulnerabilidad se explota utilizando el protocolo Netlogon (MS-NRPC).

Productos Afectados

Windows Server 2008 R2, sistemas basados en x64, Service Pack 1
Windows Server 2008 R2, sistemas basados en x64, 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 1903 (Server Core Installation)
Windows Server version 1909 (Server Core Installation)
Windows Server version 2004 (Server Core Installation)

Mitigación

Aplicar parche desarrollado por Microsoft que implementa defensa por capas (Defense-in-depth) para que equipos agregados al dominio utilicen las medidas de seguridad del protocolo Netlogon.

Enlaces

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-1472
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-1472