Alerta de seguridad cibernética	9VSA21-00399-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	2 de marzo de 2021
Última revisión	2 de marzo de 2021

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 información sobre una vulnerabilidad que afecta a Red Hat Enterprise Linux 6 Extended Lifecycle Support.

Este informe incluye las medidas de mitigación, consistentes en instalar la última actualización de los productos afectados.

Vulnerabilidades

CVE-2020-8625

Impactos

La vulnerabilidad permite a un atacante remoto ejecutar código arbitrario en el sistema objetivo. La vulnerabilidad existe debido a un error de límites de memoria dentro de la implementación SPNEGO en la extensión GSS-TSIG. Un atacante remoto puede enviar una solicitud DNS especialmente diseñada al servidor, detonar corrupción de memoria en el sistema objetivo.

Productos Afectados

Red Hat Enterprise Linux Server Extended Life Cycle Support (para sistemas IBM z) 6.0
Red Hat Enterprise Linux Server Extended Life Cycle Support 6.0
BIND (Red Hat), versiones anteriores a la 9.8.2-0.68.rc1.el6_10.10

Mitigación

Instalar las últimas actualizaciones de los productos afectados desde el sitio del proveedor.

Enlaces

https://access.redhat.com/errata/RHSA-2021:0672

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-8625

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.03.02 12:24:08 -03'00'