Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA21-00391-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Medio
TLP	Blanco
Fecha de lanzamiento original	16 de febrero de 2021
Última revisión	16 de febrero 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 la información entregada por Red Hat sobre una vulnerabilidad crítica que afecta a varios de sus productos.

Este informe incluye las medidas de mitigación, consistentes en instalar las últimas actualizaciones de los productos afectados.

Vulnerabilidad

CVE-2020-27827
CVE-2020-35498
CVE-2020-17525
CVE-2021-1721

Impacto

CVE-2020-27827 permite a un atacante remoto realizar un ataque DoS en el sistema objetivo. La vulnerabilidad existe debido a una fuga de memoria en lldpd al procesar paquetes con múltiples instancias de ciertos TLV. Un atacante remoto puede enviar tráfico especialmente diseñado al sistema y realizar un ataque DoS (de denegación de servicio).

CVE-2020-35498 permite a un atacante remoto realizar un ataque DoS en el sistema objetivo. La vulnerabilidad existe debido a una validación insuficiente de los datos ingresados por el usuario, al procesar paquetes de red. Un atacante remoto puede enviar tráfico especialmente diseñado al sistema y realizar un ataque DoS (de denegación de servicio).

CVE-2020-17525 permite a un atacante remoto realizar un ataque DoS en el sistema objetivo. Un atacante remoto no autenticado puede enviar una solicitud especialmente diseñada a una URL no existente, realizando un ataque de denegación de servicio (DoS).

CVE-2021-1721 permite a un atacante remoto realizar un ataque DoS en el sistema objetivo. La vulnerabilidad existe debido a una validación insuficiente de lo ingresado por el usuario en .NET Core y Visual Studio. Un atacante remoto puede enviar tráfico especialmente diseñado al sistema y realizar un ataque DoS (de denegación de servicio).

Productos Afectados

openvswitch2.13 (Red Hat package): 2.13.0-71.el8fdp, 2.13.0-72.el8fdp
dotnet5.0 (Red Hat package): 5.0.102-2.el8_3
Red Hat Enterprise Linux Fast Datapath: 8.
Red Hat Enterprise Linux for ARM 64 - Extended Update Support: 8.1
Red Hat Enterprise Linux for Power, little endian - Extended Update Support: 8.1
Red Hat Enterprise Linux for x86_64 - Extended Update Support: 8.1
Red Hat Enterprise Linux Server - Update Services for SAP Solutions: 8.1
Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions: 8.1
Red Hat Enterprise Linux for x86_64: 8.0
Red Hat Enterprise Linux Server - TUS: 8.2

Mitigación

Instalar las respectivas actualizaciones desde el sitio del proveedor.

Enlaces

https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-1721
https://subversion.apache.org/security/CVE-2020-17525-advisory.txt
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-27827
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-35498
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-17525
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-1721

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.02.16 17:21:48 -03'00'