Alerta de Seguridad Cibernética

Alerta de seguridad cibernética	9VSA22-00625-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	28 de abril de 2022
Última revisión	28 de abril de 2022

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 CSIRT de Gobierno. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, comparte información sobre dos nuevas vulnerabilidades descubiertas en Linux, apodadas colectivamente “Nimbuspwn”.

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

Vulnerabilidades

CVE-2022-29799
CVE-2022-29800

Impacto

CVE-2022-29799
CVE-2022-29800

Escalamiento de privilegios: ambas vulnerabilidades pueden ser usadas en conjunto para ganar privilegios de root en los sistemas afectados, y en conjunto con otras vulnerabilidades, vector para el acceso root de malware y ransomware, por ejemplo.

Productos afectados

Varias distribuciones Linux no especificadas por los descubridores de las vulnerabilidades (Microsoft). Algunas de las que han sido a conocer por sus responsables son:
Linux Mint
Debian Buster 2.0-2
Debian Bullseye 2.1-2

Debian Bookworm 2.1-2
Debian Sid 2.1-2

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Enlaces

https://www.microsoft.com/security/blog/2022/04/26/microsoft-finds-new-elevation-of-privilege-linux-vulnerability-nimbuspwn/
https://www.helpnetsecurity.com/2022/04/27/cve-2022-29799-cve-2022-29800/
https://security-tracker.debian.org/tracker/CVE-2022-29799
https://ubuntu.com/security/CVE-2022-29799
https://ubuntu.com/security/CVE-2022-29800
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-29800

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.04.28 10:38:23 -04'00'