Alerta de seguridad cibernética	9VSA23-00869-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	25 de julio de 2023
Última revisión	25 de julio de 2023

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 CSIRT de Gobierno comparte información de una vulnerabilidad de crítica que afecta a Mikrotik RouterOS.

Vulnerabilidades

CVE-2023-30799

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-30799: Vulnerabilidad de escalamiento de privilegios. Un atacante remoto y autenticado puede escalar privilegios de admin a super-admin en la interfaz HTTP o Winbox. El atacante puede abusar esta vulnerabilidad para ejecutar código arbitrario en el sistema. CVSS: 9.1.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

MikroTik RouterOS stable anteriores a la versión 6.49.7 y long-term hasta la 6.48.6.

Enlaces

https://vulncheck.com/blog/mikrotik-foisted-revisited
https://nvd.nist.gov/vuln/detail/CVE-2023-30799
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-30799

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.07.26 16:24:26 -04'00'