Alerta de seguridad cibernética	9VSA23-00839-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Crítico
TLP	Blanco
Fecha de lanzamiento original	30 de mayo de 2023
Última revisión	30 de mayo 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 crítica que afecta a Barracuda Email Security Gateway y que fue recientemente parchada.

Vulnerabilidades

CVE-2023-2868

Impacto

Vulnerabilidades críticas

CVE-2023-2868: Vulnerabilidad de inyección remoto de comandos en Barracuda Email Security Gateway versiones 5.1.3.001 a 9.2.0.006. La vulnerabilidad surgió de una validación incompleta de inputs a los archivos .tar.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

Barracuda Email Security Gateway versiones 5.1.3.001 a 9.2.0.006.

Enlaces

https://www.barracuda.com/company/legal/esg-vulnerability

https://nvd.nist.gov/vuln/detail/CVE-2023-2868

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-2868

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.05.30 15:34:06 -04'00'