Alerta de seguridad cibernética	9VSA23-00907-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2023
Última revisión	22 de septiembre 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 nuevas vulnerabilidades de alta severidad que afectan a software DNS de BIND, para los cuales liberaron dos parches.

Vulnerabilidades

CVE-2023-3341
CVE-2023-4236

Impacto

Vulnerabilidades de riesgo alto

CVE-2023-3341: Error de agotamiento de lotes. CVSS: 7.5.

CVE-2023-4236: El servicio nombrado puede terminar inesperadamente bajo alta carga de query de DNS-over-TLS. CVSS: 7.5.

Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

Productos afectados

BIND 9
9.2.0 -> 9.16.43
9.18.0 -> 9.18.18
9.19.0 -> 9.19.16

BIND Supported Preview Edition
9.9.3-S1 -> 9.16.43-S1
9.18.0-S1 -> 9.18.18-S1

Enlaces
https://kb.isc.org/docs/cve-2023-4236
https://kb.isc.org/docs/cve-2023-3341
https://nvd.nist.gov/vuln/detail/CVE-2023-3341
https://nvd.nist.gov/vuln/detail/CVE-2023-4236

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.09.22 17:11:02 -03'00'