Alerta de seguridad cibernética	9VSA23-00917-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2023
Última revisión	12 de octubre 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 sobre una reciente vulnerabilidad denominada HTTP/2 Rapid Reset Attack, que posibilita ataques contra el protocolo HTTP/2.

Vulnerabilidades

CVE-2023-44487

Impacto

Vulnerabilidades de riesgo crítico

CVE-2023-44487: Permite a un atacante malicioso enviar y cancelar solicitudes en rápida sucesión, sobrecargando el servidor y generando una condición de denegación de servicio (DDoS). CVSS: 7,5.

Mitigación

Instalar las respectivas actualizaciones entregadas por el respectivo proveedor.

Productos afectados

Software de:

Cloudfare
Amazon Web Services
Google Cloud
F5 (NGINX Open Source, NGINX Plus y relacionados).
Alibaba Tengine
Apache Tomcat 10.x
Swift NIO
Jetty
Debian
Red Hat
Ubuntu

Microsoft
Netty

Entre otros.

Enlaces

https://www.cloudflare.com/learning/ddos/application-layer-ddos-attack/
https://aws.amazon.com/es/security/security-bulletins/AWS-2023-011/
https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps
https://cloud.google.com/blog/products/identity-security/how-it-works-the-novel-http2-rapid-reset-ddos-attack
https://github.com/alibaba/tengine/issues/1872
https://tomcat.apache.org/security-10.html#Fixed_in_Apache_Tomcat_10.1.14
https://www.f5.com/company/blog/http-2-rapid-reset-attack-impacting-f5-nginx-products
https://my.f5.com/manage/s/article/K000137106
https://forums.swift.org/t/swift-nio-http2-security-update-cve-2023-44487-http-2-dos/67764/2
https://github.com/jetty/jetty.project/releases/tag/jetty-11.0.17
https://www.debian.org/security/2023/dsa-5522
https://access.redhat.com/security/cve/cve-2023-44487
https://ubuntu.com/security/CVE-2023-44487
https://msrc.microsoft.com/update-guide/releaseNote/2023-Oct
https://netty.io/news/2023/10/10/4-1-100-Final.html
https://nvd.nist.gov/vuln/detail/CVE-2023-44487
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2023-44487

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.12 17:02:57 -03'00'