

Alerta de seguridad cibernética	9VSA22-00696-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	23 de agosto de 2022
Última revisión	23 de agosto 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, CSIRT de Gobierno, comparte información sobre una vulnerabilidad de alto riesgo en programas que utilizan el firewall PAN-OS de Palo Alto.

## Vulnerabilidades

CVE-2022-0028

## Impacto

### Vulnerabilidades de alto riesgo

CVE-2022-0028: Esta vulnerabilidad puede ser usado por agentes maliciosos remotos para realizar un ataque de denegación de servicio (DoS) amplificado y reflejado sin tener que autenticar sistemas objetivo.

### Productos afectados

Productos que usan el software de firewall PAN-OS como los aparatos de las series PA, VM y CN. Versiones de PAN-OS vulnerables a ataques incluyen PAN-OS anteriores a 10.2.2-h2, 10.1.6-h6, 10.0.11-h1, 9.1.14-h4, 9.0.16-h3 y 8.1.23-h1.

### Mitigación

Instalar las respectivas actualizaciones entregadas por el proveedor.

### Enlaces

<https://security.paloaltonetworks.com/CVE-2022-0028>

<https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-0028>