Alerta de seguridad cibernética	9VSA24-00969-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	30 de enero de 2024
Última revisión	30 de enero de 2024

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 vulnerabilidades que afectan a productos WatchGuard y Panda Security.

Vulnerabilidades

CVE-2023-6330
CVE-2023-6331
CVE-2023-6332

Impacto

Vulnerabilidades de riesgo medio:

CVE-2023-6330: Vulnerabilidad que permite provocar situación de denegación de servicio. CVSS: 6.4.
CVE-2023-6331: Vulnerabilidad que permite provocar situación de denegación de servicio. CVSS: 6.4.
CVE-2023-6332: Vulnerabilidad que permite acceder a datos sensibles, o encadenarla a otras vulnerabilidades para realizar una explotación más sofisticada y de mayor impacto. CVSS: 4.1.

Mitigación

Actualizar Panda Dome a la versión 22.02.01.
Actualizar WatchGuard EPDR y AD360 a 8.0.22.0023.

Productos afectados

WatchGuard EPDR (EPP, EDR, EPDR) y Panda AD360 hasta la versión 8.00.22.0023
Panda Dome hasta la versión 22.02.01 (Essential, Advanced, Complete y Premium).

Enlaces

https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00001
https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00002
https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2024-00003

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2024.01.30 15:37:00 -03'00'