Alerta de seguridad cibernética	9VSA24-00984-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
TLP	Blanco
Fecha de lanzamiento original	13 de marzo de 2024
Última revisión	13 de marzo 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 las vulnerabilidades parchadas por Fortinet para FortiOS y FortiProxy.

Vulnerabilidades

CVE-2023-42789
CVE-2023-42790
CVE-2024-23112
CVE-2023-46717

Impacto

Vulnerabilidades de riesgo crítico:

CVE-2023-42789: Vulnerabilidad de escritura fuera de los límites de la memoria en FortiOS y FortiProxy. CVSS: 9.3.

CVE-2023-42790: Vulnerabilidad de desborde de buffer basado en lotes en FortiOS y FortiProxy. CVSS: 9.3.

Mitigación

Actualizar los programas afectados a sus versiones reparadas.

FortiOS versión 7.4.2 o superior.
FortiOS versión 7.2.6 o superior.
FortiOS versión 7.0.13 o superior.
FortiOS versión 6.4.15 o superior.
FortiOS versión 6.2.16 o superior.
FortiProxy versión 7.4.1 o superior.
FortiProxy versión 7.2.7 o superior.

FortiProxy versión 7.0.13 o superior.
FortiProxy versión 2.0.14 o superior.

Fortinet en el Q3/23 remedió este problema en FortiSASE versión 23.3.b, por lo que los usuarios no necesitan realizar ninguna acción.

Productos afectados

FortiOS versiones 7.4.0 a 7.4.1
FortiOS versiones 7.2.0 a 7.2.5
FortiOS versiones 7.0.0 a 7.0.12
FortiOS versiones 6.4.0 a 6.4.14
FortiOS versiones 6.2.0 a 6.2.15
FortiProxy versiones 7.4.0
FortiProxy versiones 7.2.0 a 7.2.6
FortiProxy versiones 7.0.0 a 7.0.12
FortiProxy versiones 2.0.0 a 2.0.13

Enlaces

https://www.fortiguard.com/psirt/FG-IR-23-328
https://www.fortiguard.com/psirt/FG-IR-24-013
https://www.fortiguard.com/psirt/FG-IR-23-424