Alerta de seguridad cibernética	9VSA20-00328-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	28 de noviembre de 2020
Última revisión	28 de noviembre de 2020

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 equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática, CSIRT, comparte la información obtenida del PSIRT de Fortinet respecto a vulnerabilidad que afecta a FortiOS y está siendo explotada actualmente. El presente informe incluye la respectiva medida de mitigación.

Vulnerabilidad

CVE-2018-13379

Es posible descargar el sistema de archivos de FortiOS sin autenticación a través de peticiones de recursos HTTP especialmente diseñadas, gracias a una vulnerabilidad de tipo ruta transversal en el portal web VPN SSL de FortiOS.

Productos Afectados

FortiOS desde la versión 6.0.0 hasta la 6.0.4, desde la 5.6.3 hasta la 5.6.7 y desde la 5.4.6 hasta la 5.4.12.
Solo si el servicio VPN SSL (modo web o modo túnel) se encuentra habilitado.

Mitigación

La vulnerabilidad fue mitigada en la versión 5.4.13, 5.6.8, 6.0.5 y 6.2.0 de FortiOS.
Se recomienda actualizar las últimas versiones disponibles.

Enlaces

https://www.fortiguard.com/psirt/FG-IR-18-384
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-13379