Alerta de seguridad informática	9VSA20-00120-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de enero de 2020
Última revisión	14 de enero 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 información obtenida de Fortinet, referente a una vulnerabilidad que afecta a Fortinet FortiSIEM, la cual de ser explotada permitiría a un atacante remoto obtener credenciales embebidas en el sistema y comprometerlo completamente. Este informe incluye la respectiva mitigación.

Vulnerabilidad

CVE-2019-16153

Impacto

La vulnerabilidad “hard-coded password” en la base de datos de FortiSIEM permitiría a un atacante remoto y sin autenticación acceder al dispositivo mediante el uso de contraseñas estáticas. La explotación de esta vulnerabilidad podría comprometer completamente al sistema.

Productos Afectados

Todas las versiones de Fortinet FortiSIEM desde la 5.0.0 hasta la 5.2.5.

Mitigación

Se debe actualizar a la versión 5.2.6 o superior.

Enlaces

https://fortiguard.com/psirt/FG-IR-19-195
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-16153

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.01.14 15:11:13 -03'00'