Alerta de seguridad informática	9VSA20-00171-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de abril de 2020
Última revisión	03 de abril 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 entregada por Grafana referente a vulnerabilidad que afecta a su software de visualización de datos. El presente informe incluye la respectiva medida de mitigación.

VULNERABILIDAD

CVE-ID N/A
CWE-79

CWE-79

Impacto

Debido a la insuficiente sanitización de datos entregados por el usuario en el dashboard “snapshots”, un atacante remoto podría engañar a una persona para que esta acceda a un enlace especialmente diseñado y así poder realizar un ataque cross-site scripting. La explotación de esta vulnerabilidad le permitiría al atacante robar información potencialmente sensible, realizar ataques phishing, cambiar la apariencia del sitio web, entre otros.

Productos Afectados

Grafana desde la versión 6.0.0 hasta la versión 6.7.1.

Mitigación

Actualizar a la versión 6.7.2 de Grafana.

Enlace

https://github.com/grafana/grafana/releases/tag/v6.7.2

https://github.com/grafana/grafana/pull/23254/commits/7a5f6f6e9ba2ea20e8b931ec9c3a4d83db34cebc