Alerta de seguridad cibernética	9VSA20-00193-01
Clase de alerta	Vulnerabilidad
Tipo de incidente	Sistema y/o Software Abierto
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	29 de abril de 2020
Última revisión	29 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-2020-12245

CVE-2020-12245

Debido a la insuficiente sanitización de datos ingresados por el usuario en los parámetros "columna.title" o "cellLinkTooltip", un atacante remoto podría engañar a una víctima para que acceda a un enlace especialmente diseñado, y así lograr ejecutar código script y HTML mediante la explotación de la vulnerabilidad Cross-site Scripting (XSS) en el contexto del sitio vulnerable.
La explotación exitosa de esta vulnerabilidad permitiría al atacante cambiar el aspecto del sitio web, robar información potencialmente sensible y engañar a la víctima para que descargue malware.

Producto Afectado

Grafana versiones 6.7.0, 6.7.1 y 6.7.2.

Mitigación

Actualizar a la versión 6.7.3 de Grafana.

Enlaces

https://community.grafana.com/t/release-notes-v6-7-x/27119
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-12245

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.04.29 15:00:08 -04'00'