# Boletín de alerta

**Boletín Nro.:**
**Fecha de publicación:** 25/04/2025
**Tema:** Alerta 2025-30 Vulnerabilidades Críticas en Grafana
**Traffic Light Protocol (TLP):** Amber

## Producto(s) afectado(s):

- Grafana OSS y Grafana Enterprise
- CVE-2025-3260: ≥ Grafana 11.6.0
- CVE-2025-2703: ≥ Grafana 11.1.0
- CVE-2025-3454: ≥ Grafana 8.0

## Descripción

Se ha publicado actualizaciones de seguridad que corrigen tres vulnerabilidades detectadas en sus productos Grafana OSS y Grafana Enterprise. Una de estas fallas, identificada como CVE-2025-3260, ha sido clasificada con gravedad alta (CVSS 8.3) y representa un riesgo importante para la confidencialidad e integridad de los paneles. Las otras dos vulnerabilidades, CVE-2025-2703 y CVE-2025-3454, han sido calificadas como de gravedad media, con puntuaciones CVSS de 6.8 y 5.0 respectivamente.

La vulnerabilidad más crítica, **CVE-2025-3260**, fue introducida en la versión 11.6.0 de Grafana y afecta a los puntos de conexión /apis/dashboard.grafana.app/*. Esta falla permite que usuarios con roles limitados, como Visores o Editores, puedan eludir los permisos asignados a nivel de panel dentro de su organización. En la práctica, esto significa que un Visor podría acceder a cualquier panel, independientemente de si tiene autorización para verlo, y un Editor podría visualizar, editar o eliminar paneles sin restricciones. Además, los entornos que tienen habilitado el acceso anónimo podrían verse aún más afectados, ya que un usuario anónimo con rol de Visor o Editor también podría acceder o modificar cualquier panel dentro de la organización. Aunque los límites entre organizaciones siguen vigentes, esta vulnerabilidad representa un riesgo alto, especialmente si la autenticación anónima está habilitada.

Por otra parte, la vulnerabilidad **CVE-2025-2703** es una falla de tipo Cross-Site Scripting (XSS) basada en DOM, detectada en el complemento de gráfico XY incluido en Grafana. Esta vulnerabilidad permite a un usuario con permisos de escritura (como los otorgados al rol general.writer) inyectar código JavaScript malicioso dentro de un gráfico. Si otro usuario visualiza ese gráfico, el código podría ejecutarse en su navegador, comprometiendo su sesión. Aunque existen políticas de seguridad de contenido (CSP) en Grafana, estas no bloquean esta vulnerabilidad en particular. Por ello, se recomienda habilitar una

funcionalidad llamada “Trusted Types” o “Tipos de Confianza”, que ayuda a prevenir este tipo de ataques al restringir cómo se puede manipular el DOM del navegador.

La tercera vulnerabilidad, **CVE-2025-3454**, fue identificada en la API de proxy de fuentes de datos de Grafana. Esta falla permite el acceso no autorizado a datos de Prometheus y Alertmanager si un atacante manipula la URL agregando una barra diagonal extra en las rutas de la API. El problema afecta a todas las versiones desde Grafana 8.0 en adelante y se presenta especialmente cuando se utilizan autenticaciones básicas o basadas en rutas. A través de esta técnica, un atacante podría leer información de fuentes de datos a las que no debería tener acceso, incluso si sus roles o permisos no lo permiten.

## Solución

Se recomienda actualizar a una de las siguientes versiones corregidas.

- **11.6.0+security-01**
- **11.5.3+security-01**
- **11.4.3+security-01**
- **11.3.5+security-01**
- **11.2.8+security-01**
- **10.4.17+security-01**

Puede encontrar las mismas en**https://grafana.com/grafana/download**

## Mitigación

En caso de que no sea posible aplicar las actualizaciones de inmediato, Grafana Labs sugiere medidas de mitigación temporales.

- Para CVE-2025-3260, se recomienda bloquear el tráfico entrante a los endpoints /apis/dashboard.grafana.app/v0alpha1, /v1alpha1 y /v2alpha1.
- Para mitigar CVE-2025-2703, se debe habilitar Trusted Types en la configuración de seguridad. Finalmente.
- Para protegerse contra CVE-2025-3454, se puede utilizar un proxy inverso que normalice y desinfecte las URLs entrantes, evitando la explotación de rutas maliciosas.

## Información adicional:

- **https://grafana.com/blog/2025/04/22/grafana-security-release-medium-and-high-severity-fixes-for-cve-2025-3260-cve-2025-2703-cve-2025-3454/**
- **Grafana aplica parches a CVE-2025-3260 y más en una actualización de seguridad crítica**