Advertencia

Incidente de instancia de GitLab en RedHat

COLCERT AD-20251006-028

TLP:CLEAR

Resumen Ejecutivo:

Red Hat ha informado sobre un acceso no autorizado a una instancia de GitLab utilizada por su equipo de consultoría, desde la cual se habrían copiado algunos datos de implementaciones y rutas de repositorios de varios clientes. Tras la evaluación realizada a la información publicada por los actores de amenaza Scattered LAPSUS$ Hunters y Crimson Collective y validaciones con algunas entidades vinculadas, se confirmó que no existe evidencia de afectación o exposición de información sensible.

No obstante, el incidente evidencia la importancia de mantener una vigilancia proactiva sobre los entornos colaborativos y de desarrollo, dado que la probabilidad de intentos futuros de explotación o reconocimiento derivados de incidentes similares se mantiene moderada. Este evento refuerza la necesidad de fortalecer los controles de acceso, segmentación y monitoreo para anticipar riesgos en la cadena de suministro y en general en la superficie de exposición. A las entidades identificadas se les remitió información de las rutas y documentos de implementación, con el propósito de que realicen la respectiva validación interna y ajustar la postura de seguridad.

Recomendaciones para las entidades vinculadas

- **Validar con sus equipos de tecnología** y seguridad digital si se mantiene alguna integración o repositorio compartido con **Red Hat** Consulting, asegurando que todo acceso se encuentre restringido y bajo monitoreo.
- **Revisar y actualizar credenciales, tokens y claves API** que hayan sido utilizados en proyectos o implementaciones desarrolladas conjuntamente, incluso si no se evidencia compromiso directo.
- **Verificar configuraciones y documentación técnica entregada o almacenada en repositorios compartidos**, garantizando que no contenga información sensible o reutilizable.
- **Fortalecer los controles de acceso y segmentación en entornos de desarrollo y pruebas**, minimizando la exposición de infraestructuras o credenciales en proyectos externos.
- **Implementar monitoreo continuo y revisión de logs**, con especial atención a conexiones o actividades provenientes de direcciones IP o usuarios inusuales.
- **Aplicar de forma oportuna los parches de seguridad** y actualizaciones publicadas por los proveedores, en especial para plataformas de colaboración y repositorios de código.
- **Adoptar contraseñas robustas y autenticación multifactor (MFA)** en todos los servicios críticos o con acceso a información corporativa o sensible.
- **Estar atentos a intentos de ingeniería social, correos de *phishing* o suplantación de entidades** que busquen aprovechar el incidente para distribuir enlaces o archivos maliciosos.

Fuentes

Red Hat, 3 de octubre de 2025, "Security update: Incident related to Red Hat Consulting GitLab instance", fuente oficial de Red Hat (conocimiento - anuncio de incidente).
https://access.redhat.com/articles/7132207
Reporte responsable de vulnerabilidades - Ciudanía.

NIVEL DE RIESGO

MEDIO