Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

RED HAT CONFIRMA INCIDENTE DE SEGURIDAD TRAS BRECHA EN SU INSTANCIA DE GITLAB

08/ 10 / 2025

CONTENIDO

INTRODUCCIÓN 3

RESUMEN 5

NOTICIA COMPLETA 5

CONTACTOS DE SOPORTE 7

INTRODUCCIÓN

En los primeros días de octubre, Red Hat confirmó haber sido víctima de un incidente de seguridad que comprometió una de sus instancias internas de GitLab, utilizada por su área de consultoría. El grupo de atacantes conocido como Crimson Collective aseguró haber robado más de 570 GB de información perteneciente a miles de repositorios y a cientos de reportes de consultoría (CERs), documentos que en muchos casos contienen detalles técnicos sensibles de clientes de alto perfil.

Aunque la compañía enfatizó que el ataque no afecta sus productos ni la cadena de suministro de software, la exposición de datos asociados a proyectos de consultoría genera preocupación en sectores clave como banca, telecomunicaciones, salud y organismos gubernamentales. Red Hat ya tomó medidas de contención, reforzó su seguridad y se encuentra notificando a los clientes potencialmente afectados mientras avanza la investigación.

RED HAT CONFIRMA INCIDENTE DE SEGURIDAD TRAS BRECHA EN SU INSTANCIA DE GITLAB

A continuación, se encuentra en cuadro de identificación de la amenaza.

ID de alerta:	DSOC-CERT_2025_10_08_1
Clasificación de alerta:	Noticia
Tipo de Impacto:	Alta
TLP (Clasificación de información):	**CLEAR**
Fecha de publicación:	08/10/2025
Es día cero (0 day):	No

RESUMEN

El ataque

Red Hat confirmó que un grupo de atacantes, que se hace llamar Crimson Collective, logró comprometer una instancia de GitLab utilizada exclusivamente por su división de consultoría. Los cibercriminales aseguran haber robado cerca de 570 GB de información comprimida, perteneciente a más de 28,000 repositorios internos de desarrollo.

Entre los datos sustraídos destacan aproximadamente 800 Customer Engagement Reports (CERs), documentos de consultoría que pueden contener información crítica sobre la infraestructura tecnológica de los clientes, configuraciones, tokens de autenticación y otros datos sensibles que, en malas manos, podrían facilitar ataques a redes corporativas.

Datos expuestos

El grupo afirmó que los informes robados corresponden a clientes de alto perfil, incluyendo entidades financieras, compañías de telecomunicaciones, cadenas minoristas, instituciones de salud y agencias gubernamentales de Estados Unidos. Entre los nombres mencionados figuran Bank of America, T-Mobile, AT&T, Walmart, Costco, la Marina de EE. UU., la FAA y la Cámara de Representantes, entre otros.

Los atacantes aseguran que hallaron credenciales, URIs de bases de datos y tokens de acceso en el código de Red Hat y en los CERs, lo que les habría permitido incluso acceder a infraestructuras de clientes.

Respuesta de Red Hat

En un comunicado oficial, Red Hat confirmó la intrusión y aclaró que la brecha se limitó a la instancia de GitLab de su área de consultoría. Según la empresa, no hay indicios de que otros servicios, productos o la cadena de suministro de software se hayan visto afectados.

Tras detectar el acceso no autorizado, la compañía tomó medidas inmediatas: revocó accesos, aisló la instancia comprometida, notificó a las autoridades y reforzó la seguridad de su entorno. Además, comenzó a contactar directamente a los clientes potencialmente afectados para proporcionar detalles sobre lo sucedido.

Intento de extorsión

Los atacantes habrían intentado extorsionar a Red Hat, pero la compañía no respondió a sus demandas. Según el grupo, sus comunicaciones fueron canalizadas como si se tratara de reportes de vulnerabilidad, lo que generó frustración en los delincuentes.

En paralelo, Crimson Collective también se adjudicó el defacement de una página de Nintendo la semana anterior, lo que refuerza su búsqueda de notoriedad en la comunidad de ciberseguridad.

Impacto y lecciones

Aunque Red Hat afirma que los CERs usualmente no contienen información personal, la exposición de especificaciones de proyectos, ejemplos de código y comunicaciones internas representa un riesgo significativo para clientes de sectores críticos.

Este incidente pone en evidencia la importancia de reforzar la seguridad en instancias autogestionadas de herramientas colaborativas como GitLab, así como la necesidad de limitar la inclusión de credenciales y datos sensibles en repositorios de código.

NOTICIA COMPLETA

https://devel.group/blog/red-hat-confirma-incidente-de-seguridad-tras-brecha-en-su-instancia-de-gitlab/

CONTACTOS DE SOPORTE

Correo electrónico: teamcti@devel.group

Teléfonos directos:

Guatemala: +(502) 2307 5757

El Salvador: +(503) 2249 4252

Honduras: +(504) 2283 5904

República Dominicana: +1 829 734 2040

WhatsApp: +(502) 5124 9536

Sitio Web: https://devel.group/