Guatemala - El Salvador - Honduras - República Dominicana

Devel
CYBERSECURITY REDEFINED

CYBER SECURITY NEWS

SECURITY OPERATIONS CENTER

Gitlab corrige vulnerabilidades en una nueva actualización.

1/julio/2022

Contenido

Introducción

En el presente boletín le damos a conocer las vulnerabilidades corregidas por GitLab en su mas reciente actualización, sugerimos prestar atención a este documento y aplicar las correcciones necesarias.

GitLab

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

ID de alerta:	DSOC-CERT_2022_07_01_02
Clasificación de alerta:	Noticia
Tipo de Impacto:	ALTO
TLP (Clasificación de información):	**WHITE**
Fecha de publicación:	07/01/2022
Es día cero (0 day):	NO

Resumen

GitLab lanzó las versiones 15.1.1, 15.0.4 y 14.10.5 para GitLab Community Edition (CE) y Enterprise Edition (EE). Este lanzamiento crítico también servirá como lanzamiento de seguridad mensual para junio.

Estas versiones contienen correcciones de seguridad importantes y se recomienda enfáticamente que todas las instalaciones de GitLab se actualicen a una de estas versiones de inmediato. GitLab.com ya está ejecutando la versión parcheada.

Tabla de Correcciones:

Título	Gravedad
Ejecución remota de comandos a través de importaciones de proyectos	crítico
XSS en la integración de ZenTao que afecta a las instancias autohospedadas sin CSP estricto	alto

XSS en la página de configuración del proyecto	alto
Los usuarios no autorizados pueden leer variables de CI desprotegidas	alto
Omisión de la lista de IP permitida para acceder a los registros de contenedores	medio
El estado de 2FA se divulga a usuarios no autenticados	medio
Restringir la membresía mediante la omisión del dominio de correo electrónico	medio
IDOR en Centry	medio
Los reporteros pueden gestionar problemas en el seguimiento de errores	medio
Variables de CI proporcionadas a corredores fuera del rango de IP restringido de un grupo	medio
Denegación de servicio de expresiones regulares a través de respuestas de servidores web maliciosos	medio
Lectura no autorizada para el repositorio conan	bajo
Vulnerabilidad de redirección abierta	bajo
Las etiquetas de grupo se pueden editar a través del subproyecto	bajo
Títulos de lanzamiento visibles para cualquier usuario si los hitos del grupo están asociados con cualquier lanzamiento de proyecto	bajo
La información del trabajo se filtra a los usuarios que anteriormente eran mantenedores a través del punto final de la API Runner Jobs	medio

Hacemos énfasis en la vulnerabilidad critica:

Ejecución remota de comandos a través de importaciones de proyectos.

Se ha descubierto un problema crítico en GitLab que afecta a todas las versiones a partir de la 14.0 anterior a la 14.10.5, la 15.0 anterior a la 15.0.4 y la 15.1 anterior a la 15.1.1, en la que un usuario autorizado podría importar un proyecto creado con fines malintencionados que condujera a la ejecución remota de código. Este es un problema de gravedad crítica con nota de 9.9. Ahora está mitigado en la última versión y se le asigna CVE-2022-2185 .

Recomendaciones

- Se recomienda agendar una ventana de mantenimiento para poder aplicar las actualizaciones correspondientes para evitar que los actores maliciosos no puedan vulnerar sus recursos.

Noticia Completa

https://about.gitlab.com/releases/2022/06/30/critical-security-release-gitlab-15-1-1-released/

Enlaces de Descarga

GitLab: https://about.gitlab.com/update

GitLab Runner: https://docs.gitlab.com/runner/install/linux-repository.html#updating-the-runner

CONTACTOS DE SOPORTE

Correo electrónico: cert@develsecurity.com

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://www.devel.group/reporta-un-incidente