CONCIBER
Comité Nacional de Seguridad Cibernética

ALERTA

Vulnerabilidad de software

Fecha: **02/05/2024**

Problemática: **Múltiples vulnerabilidades afectan al servicio de GitLab**

Correlativo: **AC-0020**

Institución / Sector: **Público y Privado**

CONTEXTO

La Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA) ha reportado que actores de amenazas se encuentran explotando activamente una falla crítica que afecta al servicio GitLab, proveedor de un repositorio Git de código abierto basado en la nube.

Las vulnerabilidades registradas como CVE-2023-5356, CVE-2023-4812, CVE-2023-6955 y CVE-2023-2030 clasificadas de alta gravedad, facilitan la apropiación de cuentas mediante el envío de correos electrónicos de restablecimiento de contraseña a una dirección de correo electrónico no verificada

Nivel de priorización

Prioridad Urgente / No Urgente	Actualización Seguimiento/Preventiva/Resiliente
Urgente	**Preventiva**

Matriz de Evaluación

Riesgo Alto/ Medio/ Bajo	Nivel de Afectación		
	Integridad	Disponibilidad	Confidencialidad
Alto	**Alta**	**Alta**	**Alta**

PRODUCTOS VULNERABLES

GitLab

- **16.5.6**
- **16.6.4**
- **16.7.2**
- **16.1.6**
- **16.2.9**
- **16.3.7**
- **16.4.5**

RECOMENDACIONES

Ejecutar las actualizaciones recomendadas por el fabricante para corregir la falla presentada.

REFERENCIAS

The hacker News
https://thehackernews.com/2024/05/cisa-warns-of-active-exploitation-of.html

MITIGA
https://www.mitiga.io/blog/understanding-gitlabs-security-threats-and-strengthening-your-preparedness