| | ALERTA INTEGRADA DE SEGURIDAD DIGITAL N°291 | Fecha: 06-12-2023 |
|---|---|---|
| | | Página: 8 de 13 |

| | | | |
|---|---|---|---|
| Componente que reporta | **DIRECCIÓN NACIONAL DE INTELIGENCIA** | | |
| Nombre de la alerta | Vulnerabilidades en el lenguaje de programación Go | | |
| Tipo de Ataque | Explotación de vulnerabilidades conocidas | Abreviatura | EVC |
| Medios de propagación | Red, Internet | | |
| Código de familia | H | Código de Sub familia | H01 |
| Clasificación temática familia | Intento de intrusión | | |

Descripción

**1. ANTECEDENTES:**

Se ha reportado dos vulnerabilidades de severidad **MEDIA** de tipo agotamiento de recursos y falta de cifrado de datos confidenciales en el lenguaje de programación Go. La explotación exitosa de estas vulnerabilidades podría permitir a un atacante remoto realizar un ataque de denegación de servicio (DoS) y MitM.

**2. DETALLES:**

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-39326 de tipo agotamiento de recursos, existe debido a que la aplicación no controla adecuadamente el consumo de recursos internos al manejar solicitudes HTTP fragmentadas. Un atacante remoto puede enviar solicitudes HTTP especialmente diseñadas al servidor y consumir recursos de memoria excesivos.

La vulnerabilidad de severidad **media**, identificada por MITRE como CVE-2023-45285 de tipo falta de cifrado de datos confidenciales, existe debido a una alternativa a git inseguro. El uso de "go get" para buscar un módulo con el sufijo ".git" puede recurrir inesperadamente al protocolo inseguro "git://" si el módulo no está disponible a través de "https://" seguro y git+ssh:// "protocolos, incluso si GOINSECURE no está configurado para dicho módulo. Esto solo afecta a los usuarios que no están usando el proxy del módulo y están recuperando módulos directamente (es decir, OPROXY=off).

**A. Productos afectados:**

- Go programming language: 1.20 - 1.21.4

**3. RECOMENDACIÓN:**

- Actualizar el producto afectado a la última versión de software disponible que aborda estas vulnerabilidades.

| | |
|---|---|
| Fuente de Información: | • hxxp://github.com/golang/go/issues/64433<br>• hxxp://groups.google.com/g/golang-announce/c/iLGK3x6yuNo |