Informe de Seguridad - AlamOps

Fecha del Reporte: 10/04/2025

Índice

---

1. Resumen de Información WHOIS

- **Dominio:** alamops.com
- **ID de Dominio:** 2923836650_DOMAIN_COM-VRSN
- **Registrador:** GoDaddy.com, LLC (http://www.godaddy.com)
- **Servidor WHOIS:** whois.godaddy.com
- **Fechas Clave:**
  - Creación: 09/10/2024
  - Última Actualización: 09/10/2024
  - Expiración: 09/10/2027
- **Estados del Dominio:**
  - `clientDeleteProhibited`
  - `clientRenewProhibited`
  - `clientTransferProhibited`
  - `clientUpdateProhibited`
- **Servidores de Nombre:**
  - NS67.DOMAINCONTROL.COM
  - NS68.DOMAINCONTROL.COM
- **DNSSEC:** No firmado (unsigned)

---

2. Información del Registrante

- **Nombre:** Registration Private
- **Organización:** Domains By Proxy, LLC
- **Dirección:** 100 S. Mill Ave, Suite 1600, Tempe, Arizona, 85281, US
- **Teléfono:** +1.4806242599
- **Email:** Contactar vía GoDaddy

---

3. Resultados de Escaneo Nmap

- **Fecha:** 10/04/2025
- **IP:** 3.64.114.185
- **Hostname:** ec2-3-64-114-185.eu-central-1.compute.amazonaws.com

Puertos Abiertos y Servicios Detectados:

- **22/tcp - SSH**
  - Servicio: OpenSSH 9.6p1 (Ubuntu 3ubuntu13.8)
  - Claves Host: ED25519, ECDSA
- **80/tcp - HTTP**
  - Servicio: nginx 1.24.0 (Ubuntu)
  - Observación: Redirección a HTTPS
- **443/tcp - HTTPS**
  - Servicio: nginx 1.24.0 (Ubuntu)
  - Certificado SSL: Válido (19/02/2025 – 20/05/2025)
  - CN/SAN: alamops.com, www.alamops.com
  - Título: *AlamOps - Expertos en Cloud Computing*

Sistema Operativo Detectado: Linux (`cpe:/o:linux:linux_kernel`)

---

4. Análisis de Seguridad con Nikto

- **URL Analizada:** https://alamops.com
- **Servidor Web:** nginx/1.24.0 (Ubuntu)
- **Certificado SSL:** Let's Encrypt

Hallazgos de Seguridad:

- ❌ Falta cabecera `X-Frame-Options` (protección contra clickjacking).
- ❌ Falta cabecera `HTTP Strict-Transport-Security (HSTS).`
- ❌ Falta cabecera `X-Content-Type-Options` (protección contra MIME-sniffing).

Recomendaciones:

- Implementar cabeceras de seguridad faltantes.
- Actualizar configuraciones del servidor periódicamente.

---

5. Enumeración de Subdominios

- **Herramienta:** Sublist3r

- **Subdominios Identificados (7):**
  - www.alamops.com
  - api-dev.alamops.com
  - grafana.alamops.com
  - iac-dev.alamops.com
  - jenkins.alamops.com
  - pve.alamops.com
  - registry.alamops.com

Hallazgos:

- Subdominios críticos detectados (ej. `grafana`, `jenkins`).
- Servicios de terceros (VirusTotal, DNSdumpster) bloquearon solicitudes.

Recomendaciones:

- Evaluar seguridad en subdominios de gestión interna.
- Ampliar técnicas de enumeración.

---

6. Enumeración de DNS

- **Herramienta:** Amass

Registros Clave:

- **Servidores de Nombre (NS):**
  - ns68.domaincontrol.com
  - ns67.domaincontrol.com
- **Registros MX:**
  - Servidores de Google Mail (aspmx.l.google.com y alternativos)

Recomendaciones:

- Reforzar seguridad contra ataques de DNS spoofing/hijacking.
- Validar configuraciones de correo electrónico.

---

7. Resultados del Escaneo con SQLMap

- **URL Analizada:** http://alamops.com/page.php?id=1

Hallazgos:

- No se detectaron vulnerabilidades de inyección SQL en el parámetro `id`.
- Redirección a HTTPS implementada.
- Ausencia de WAF/IPS detectado.

Recomendaciones:

- Implementar WAF/IPS para protección adicional.
- Realizar pruebas con técnicas avanzadas (`--tamper=space2comment`).

---

8. Conclusiones y Recomendaciones Generales

Prioridad Alta:

- Corregir cabeceras de seguridad faltantes (Nikto).
- Asegurar subdominios críticos (`grafana`, `jenkins`).

Prioridad Media:

- Implementar WAF/IPS.
- Validar configuraciones DNS y de correo.

Equipo de Seguridad
AlamOps - Expertos en Cloud Computing

Layth Salameh Salameh