CVE-2025-69606 — Reflected XSS in GSVoIP Web Panel

> **Severity:** Medium | **CWE:** CWE-79 | **Auth Required:** No | **Vector:** Remote

Summary

A **Reflected Cross-Site Scripting (XSS)** vulnerability was identified in the **GSVoIP Web Panel (v2.0.90)**. The `msg` parameter of the error endpoint does not sanitize user-controlled input before reflecting it in the HTML response, allowing arbitrary JavaScript execution in the victim's browser.

Affected Product

Field	Details
Product	GSVoIP Web Panel
Version	2.0.90 (likely earlier versions)
Vendor	Solutions VoIP (GS Solutions)

Field	Details
CWE	CWE-79 — Cross-Site Scripting
Attack Vector	Remote / Network
Authentication	Not required

Vulnerable Endpoint

```
GET /painel/gateways.php/error?msg=<payload>
```

The `msg` parameter is reflected directly in the HTML response without sanitization or output encoding.

Proof of Concept

Payload

```
https://{TARGET}/painel/gateways.php/error?
msg=%3Cscript%3Ealert(1)%3C%2Fscript%3E
```

Decoded:

```
<script>alert(1)</script>
```

Result

When the crafted URL is accessed, the injected payload executes in the victim's browser:

```
alert(1)
```

Attack Scenario

1. The attacker crafts a malicious URL containing the XSS payload in the `msg` parameter.
2. The victim is tricked into clicking the link (via phishing, social engineering, etc.).
3. The page loads and the injected JavaScript executes in the victim's browser context — **no authentication required**.

Impact

- Arbitrary JavaScript execution in the victim's browser
- Session hijacking via cookie theft
- Phishing and social engineering attacks
- Sensitive data exfiltration
- Content defacement within the application context

Recommendations

- **Output encoding:** Encode all user-supplied input before rendering it in HTML responses (HTML entity encoding at minimum).
- **Secure templating:** Use a templating engine with auto-escaping enabled.
- **Content Security Policy (CSP):** Implement a strict CSP with restrictive `script-src` directives.
- **Input validation:** Reject or strip parameters containing HTML tags or script sequences at the input layer.

Disclosure Timeline

Step	Event
1	Vulnerability discovered and reported by Luiz Eduardo
2	CVE assigned: `CVE-2025-69606`
3	Public disclosure

Credits

Discovered and reported by **Luiz Eduardo**

Releases

No releases published

Packages

No packages published

Contributors 1

Razielx64 Eduardo