



# CVE-2025-69606

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

## Summary

|                 |                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2025-69606                                                                                                            |
| State           | PUBLISHED                                                                                                                 |
| Assigner        | mitre                                                                                                                     |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                              |
| Published       | 2026-05-01 18:16:13 UTC                                                                                                   |
| Updated         | 2026-05-07 15:15:06 UTC                                                                                                   |
| Description     | Cross-Site Scripting (XSS) vulnerability was discovered in the GSVoIP web panel version 2.0.90. The `msg` parameter in th |

## Risk And Classification

Primary CVSS: v3.1 6.1 MEDIUM from ADP

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

EPSS: 0.000490000 probability, percentile 0.151080000 (date 2026-05-12)

Problem Types: CWE-79 | n/a | CWE-79 CWE-79 Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')

| Version | Source                               | Type      | Score | Severity | Vector                                       |
|---------|--------------------------------------|-----------|-------|----------|----------------------------------------------|
| 3.1     | ADP                                  | DECLARED  | 6.1   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N |
| 3.1     | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | Secondary | 6.1   | MEDIUM   | CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N |

## CVSS v3.1 Breakdown

Attack Vector

Network

Attack Complexity

Low

Privileges Required

None

User Interaction

Required

Scope

Changed

Confidentiality

Low

ntegrity

Low

Availability

None

CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:L/A:N

Vendor Declared Affected Products

| Source | Vendor | Product | Version      | Platforms     |
|--------|--------|---------|--------------|---------------|
| CNA    | Na     | N/a     | affected n/a | Not specified |

References

| Reference                                           | Source                               | Link                      | Tags         |
|-----------------------------------------------------|--------------------------------------|---------------------------|--------------|
| www.solutionsvoip.com.br                            | cve@mitre.org                        | www.solutionsvoip.com.br  |              |
| github.com/Razielx64/CVE-2025-69606-GSVoIP-XSS      | 134c704f-9b21-4f2e-91b3-4a467353bcc0 | github.com                |              |
| sip2.solutionsvoip.com.br/painel/gateways.php/error | cve@mitre.org                        | sip2.solutionsvoip.com.br |              |
| CVE Program record                                  | CVE.ORG                              | www.cve.org               | canonical    |
| NVD vulnerability detail                            | NVD                                  | nvd.nist.gov              | canonical, a |

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.