



# CVE-2009-0806

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

## Summary

|                 |                                                                                                                           |
|-----------------|---------------------------------------------------------------------------------------------------------------------------|
| CVE             | CVE-2009-0806                                                                                                             |
| State           | PUBLISHED                                                                                                                 |
| Assigner        | mitre                                                                                                                     |
| Source Priority | CVE Program / NVD first with legacy fallback                                                                              |
| Published       | 2009-03-04 17:30:02 UTC                                                                                                   |
| Updated         | 2026-04-23 00:35:47 UTC                                                                                                   |
| Description     | Unspecified vulnerability in OpenGoo before 1.2.1 allows remote authenticated users to modify their own permissions via u |

## Risk And Classification

Primary CVSS: v2.0 6.5 from nvd@nist.gov

AV:N/AC:L/Au:S/C:P/I:P/A:P

Problem Types: CWE-264 | n/a

## CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:S/C:P/I:P/A:P

## NVD Known Affected Configurations (CPE 2.3)

| Type        | Vendor  | Product | Version | Update | Edition | Language |
|-------------|---------|---------|---------|--------|---------|----------|
| Application | Opengoo | Opengoo | 0.1     | alpha  | All     | All      |

|             |         |         |       |        |     |     |
|-------------|---------|---------|-------|--------|-----|-----|
| Application | Opengoo | Opengoo | 0.2   | alpha  | All | All |
| Application | Opengoo | Opengoo | 0.3   | alpha  | All | All |
| Application | Opengoo | Opengoo | 0.4   | alpha  | All | All |
| Application | Opengoo | Opengoo | 0.5   | beta   | All | All |
| Application | Opengoo | Opengoo | 0.5.1 | beta   | All | All |
| Application | Opengoo | Opengoo | 0.5.2 | beta   | All | All |
| Application | Opengoo | Opengoo | 0.6.0 | All    | All | All |
| Application | Opengoo | Opengoo | 0.6.2 | All    | All | All |
| Application | Opengoo | Opengoo | 0.6.4 | All    | All | All |
| Application | Opengoo | Opengoo | 0.6.6 | All    | All | All |
| Application | Opengoo | Opengoo | 0.7   | All    | All | All |
| Application | Opengoo | Opengoo | 0.7.1 | All    | All | All |
| Application | Opengoo | Opengoo | 0.8   | All    | All | All |
| Application | Opengoo | Opengoo | 0.9   | All    | All | All |
| Application | Opengoo | Opengoo | 0.9   | rc2    | All | All |
| Application | Opengoo | Opengoo | 0.9.1 | All    | All | All |
| Application | Opengoo | Opengoo | 0.9.2 | All    | All | All |
| Application | Opengoo | Opengoo | 1.0   | All    | All | All |
| Application | Opengoo | Opengoo | 1.0   | rc1    | All | All |
| Application | Opengoo | Opengoo | 1.0   | rc2    | All | All |
| Application | Opengoo | Opengoo | 1.0   | rc3    | All | All |
| Application | Opengoo | Opengoo | 1.1   | All    | All | All |
| Application | Opengoo | Opengoo | 1.1   | beta   | All | All |
| Application | Opengoo | Opengoo | 1.1   | rc1    | All | All |
| Application | Opengoo | Opengoo | 1.1   | rc2    | All | All |
| Application | Opengoo | Opengoo | 1.2   | beta   | All | All |
| Application | Opengoo | Opengoo | 1.2   | beta_2 | All | All |
| Application | Opengoo | Opengoo | 1.2   | rc1    | All | All |
| Application | Opengoo | Opengoo | 1.2   | rc2    | All | All |
| Application | Opengoo | Opengoo | All   | All    | All | All |

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

| References |        |  |  |  |  |  |
|------------|--------|--|--|--|--|--|
| Reference  | Source |  |  |  |  |  |

| Reference                                                                                               | Source                      |
|---------------------------------------------------------------------------------------------------------|-----------------------------|
| OpenGoo User Permissions Security Bypass Vulnerability                                                  | af854a3a-2127-422b-91ae-364 |
| SourceForge.net: Feng Office: Your World Wide Office: Files                                             | af854a3a-2127-422b-91ae-364 |
| OpenGoo User Permissions Security Bypass - Secunia Advisories - Vulnerability Information - Secunia.com | af854a3a-2127-422b-91ae-364 |
| CVE Program record                                                                                      | CVE.ORG                     |
| NVD vulnerability detail                                                                                | NVD                         |



No vendor comments have been submitted for this CVE.

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