# CVE-2008-2069

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

## Summary

| | |
|---|---|
| **CVE** | CVE-2008-2069 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2008-05-02 23:20:00 UTC |
| **Updated** | 2018-10-11 20:39:00 UTC |
| **Description** | Buffer overflow in Novell GroupWise 7 allows remote attackers to cause a denial of service or execute arbitrary code via a l |

## Risk And Classification

**Problem Types:** CWE-119

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Application | Novell | Groupwise | 7.0 | All | All | All |
| Application | Novell | Groupwise | 7.0 | sp1 | All | All |
| Application | Novell | Groupwise | 7.0 | sp2 | All | All |
| Application | Novell | Groupwise | 7.0 | sp3 | All | All |
| Application | Novell | Groupwise | 7.0 | All | All | All |
| Application | Novell | Groupwise | 7.0 | sp1 | All | All |
| Application | Novell | Groupwise | 7.0 | sp2 | All | All |
| Application | Novell | Groupwise | 7.0 | sp3 | All | All |

## References

| Reference | Source | Li |
|---|---|---|
| SecurityFocus | BUGTRAQ | ww |
| SecurityFocus | BUGTRAQ | ww |
| SecurityReason - GroupWise 7.0 mailto: scheme buffer overflow | SREASON | se |
| Webmail : Solution de messagerie professionnelle - OVHcloud- OVH | VUPEN | ww |
| IBM X-Force Exchange | XF | ex |
| Novell GroupWise Buffer Overflow in 'mailto:' URL Handler Lets Remote Users Execute Arbitrary Code - SecurityTracker | SECTRACK | ww |

| | | |
|---|---|---|
| Novell GroupWise 'mailto' URI Handler Buffer Overflow Vulnerability | BID | ww |
| Groupwise 7.0 - 'mailto: scheme' Buffer Overflow (PoC) - Windows dos Exploit | EXPLOIT-DB | ww |
| SecurityFocus | BUGTRAQ | ww |
| CVE Program record | CVE.ORG | ww |
| NVD vulnerability detail | NVD | nv |

No vendor comments have been submitted for this CVE.

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