# CVE-2001-0867

MITRE | NVD | CVE.ORG | Print: PDF

## Summary

| | |
|---|---|
| **CVE** | CVE-2001-0867 |
| **State** | PUBLIC |
| **Assigner** | cve@mitre.org |
| **Source Priority** | CVE Program / NVD first with legacy fallback |
| **Published** | 2001-12-06 05:00:00 UTC |
| **Updated** | 2017-10-10 01:29:00 UTC |
| **Description** | Cisco 12000 with IOS 12.0 and line cards based on Engine 2 does not properly filter does not properly filter packet fragmen |

## Risk And Classification

**Problem Types:** NVD-CWE-Other

## NVD Known Affected Configurations (CPE 2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Hardware | Cisco | 12000 Router | All | All | All | All |
| Hardware | Cisco | 12000 Router | All | All | All | All |

## References

| Reference | Source | L |
|---|---|---|
| Cisco Security Advisory: Multiple vulnerabilities in Access Control List implementation for Cisco 12000 Series Internet Router | CISCO | w |
| M-018 | CIAC | w |
| IBM X-Force Exchange | XF | e |
| 404 Not Found | OSVDB | w |
| Cisco 12000 Outgoing ACL Fragmented Packet Vulnerability | BID | w |
| CVE Program record | CVE.ORG | w |
| NVD vulnerability detail | NVD | n |

No vendor comments have been submitted for this CVE.

## Legacy QID Mappings

317196 Cisco Internetwork Operating System (IOS) Access Control List Implementation Vulnerability (cisco-sa-20011114-gsr-acl)