



CVE-2001-0867

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

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	v
M-018	CIAC	v
IBM X-Force Exchange	XF	e
404 Not Found	OSVDB	v
Cisco 12000 Outgoing ACL Fragmented Packet Vulnerability	BID	v
CVE Program record	CVE.ORG	v
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)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)