



# CVE-2006-0483

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF](#)

## Summary

<b>CVE</b>	CVE-2006-0483
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2006-01-31 20:03:00 UTC
<b>Updated</b>	2018-10-30 16:26:00 UTC
<b>Description</b>	Cisco VPN 3000 series concentrators running software 4.7.0 through 4.7.2.A allow remote attackers to cause a denial of se

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7(rel)	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.1	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.1.f	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.2	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.2.a	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7(rel\)	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.1	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.1.f	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.2	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7.2.a	All	All	All
Operating System	Cisco	Vpn 3000 Concentrator Series Software	4.7(rel\)	All	All	All
Operating System	Cisco	Vpn 3030 Concentator	4.7(rel)	All	All	All
Operating System	Cisco	Vpn 3030 Concentator	4.7.1	All	All	All
Operating System	Cisco	Vpn 3030 Concentator	4.7.1.f	All	All	All
Operating System	Cisco	Vpn 3030 Concentator	4.7.2	All	All	All

Operating System	Cisco	Vpn 3030 Concentrator	4.7.2.a	All	All	All
Operating System	Cisco	Vpn 3030 Concentrator	4.7(rel\)	All	All	All
Operating System	Cisco	Vpn 3030 Concentrator	4.7.1	All	All	All
Operating System	Cisco	Vpn 3030 Concentrator	4.7.1.f	All	All	All
Operating System	Cisco	Vpn 3030 Concentrator	4.7.2	All	All	All
Operating System	Cisco	Vpn 3030 Concentrator	4.7.2.a	All	All	All
Operating System	Cisco	Vpn 3030 Concentrator	4.7(rel\)	All	All	All

## References

Reference	Source	Link
Cisco VPN 3000 Concentrator HTTP Packet Denial of Service - Advisories - Secunia	SECUNIA	<a href="#">secun</a>
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO	<a href="#">www.</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">www.</a>
Cisco VPN 3000 Concentrator Malformed HTTP/TCP Packet Remote Denial of Service Vulnerability	BID	<a href="#">www.</a>
Cisco VPN 3000 Concentrator Vulnerable to Crafted HTTP Attack - CXSecurity.com	SREASON	<a href="#">secu</a>
IBM X-Force Exchange	XF	<a href="#">excha</a>
SecurityTracker.com Archives - Cisco VPN 3000 Concentrator Bug in HTTP Service Lets Remote Users Deny Service	SECTRACK	<a href="#">secu</a>
22754	OSVDB	<a href="#">www.</a>
CVE Program record	CVE.ORG	<a href="#">www.</a>
NVD vulnerability detail	NVD	<a href="#">nvd.n</a>

No vendor comments have been submitted for this CVE.

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

© 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](#)