



CVE-2013-6981

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

Summary

CVE	CVE-2013-6981
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-12-28 04:53:00 UTC
Updated	2016-09-15 19:24:00 UTC
Description	Cisco IOS XE 3.7S(.1) and earlier allows remote attackers to cause a denial of service (Packet Processor crash) via fragme

Risk And Classification

Problem Types: CWE-20

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios Xe	2.5(.0)	All	All	All
Operating System	Cisco	ios Xe	2.5\(.0\)	All	All	All
Operating System	Cisco	ios Xe	2.6(.0)	All	All	All
Operating System	Cisco	ios Xe	2.6(.1)	All	All	All
Operating System	Cisco	ios Xe	2.6(.2)	All	All	All
Operating System	Cisco	ios Xe	2.6\(.0\)	All	All	All
Operating System	Cisco	ios Xe	2.6\(.1\)	All	All	All
Operating System	Cisco	ios Xe	2.6\(.2\)	All	All	All
Operating System	Cisco	ios Xe	3.1s(.0)	All	All	All
Operating System	Cisco	ios Xe	3.1s(.1)	All	All	All
Operating System	Cisco	ios Xe	3.1s(.2)	All	All	All
Operating System	Cisco	ios Xe	3.1s(.3)	All	All	All
Operating System	Cisco	ios Xe	3.1s\(.0\)	All	All	All
Operating System	Cisco	ios Xe	3.1s\(.1\)	All	All	All
Operating System	Cisco	ios Xe	3.1s\(.2\)	All	All	All
Operating System	Cisco	ios Xe	3.1s\(.3\)	All	All	All
Operating System	Cisco	ios Xe	3.2s(.0)	All	All	All

Operating System	Cisco	los Xe	3.2s(.1)	All	All	All
Operating System	Cisco	los Xe	3.2s(.2)	All	All	All
Operating System	Cisco	los Xe	3.2s(.0\)	All	All	All
Operating System	Cisco	los Xe	3.2s(.1\)	All	All	All
Operating System	Cisco	los Xe	3.2s(.2\)	All	All	All
Operating System	Cisco	los Xe	3.3s(.0)	All	All	All
Operating System	Cisco	los Xe	3.3s(.1)	All	All	All
Operating System	Cisco	los Xe	3.3s(.2)	All	All	All
Operating System	Cisco	los Xe	3.3s(.0\)	All	All	All
Operating System	Cisco	los Xe	3.3s(.1\)	All	All	All
Operating System	Cisco	los Xe	3.3s(.2\)	All	All	All
Operating System	Cisco	los Xe	3.4s(.0)	All	All	All
Operating System	Cisco	los Xe	3.4s(.1)	All	All	All
Operating System	Cisco	los Xe	3.4s(.2)	All	All	All
Operating System	Cisco	los Xe	3.4s(.3)	All	All	All
Operating System	Cisco	los Xe	3.4s(.4)	All	All	All
Operating System	Cisco	los Xe	3.4s(.5)	All	All	All
Operating System	Cisco	los Xe	3.4s(.6)	All	All	All
Operating System	Cisco	los Xe	3.4s(.0\)	All	All	All
Operating System	Cisco	los Xe	3.4s(.1\)	All	All	All
Operating System	Cisco	los Xe	3.4s(.2\)	All	All	All
Operating System	Cisco	los Xe	3.4s(.3\)	All	All	All
Operating System	Cisco	los Xe	3.4s(.4\)	All	All	All
Operating System	Cisco	los Xe	3.4s(.5\)	All	All	All
Operating System	Cisco	los Xe	3.4s(.6\)	All	All	All
Operating System	Cisco	los Xe	3.5s(.0)	All	All	All
Operating System	Cisco	los Xe	3.5s(.1)	All	All	All
Operating System	Cisco	los Xe	3.5s(.2)	All	All	All
Operating System	Cisco	los Xe	3.5s(.0\)	All	All	All
Operating System	Cisco	los Xe	3.5s(.1\)	All	All	All
Operating System	Cisco	los Xe	3.5s(.2\)	All	All	All
Operating System	Cisco	los Xe	3.6s(.0)	All	All	All
Operating System	Cisco	los Xe	3.6s(.1)	All	All	All
Operating System	Cisco	los Xe	3.6s(.2)	All	All	All
Operating System	Cisco	los Xe	3.6s(.0\)	All	All	All

Operating System	Cisco	los Xe	3.6s\(.1\)	All	All	All
Operating System	Cisco	los Xe	3.6s\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.7s\(.0\)	All	All	All
Operating System	Cisco	los Xe	3.7s\(.0\)	All	All	All
Operating System	Cisco	los Xe	2.5\(.0\)	All	All	All
Operating System	Cisco	los Xe	2.6\(.0\)	All	All	All
Operating System	Cisco	los Xe	2.6\(.1\)	All	All	All
Operating System	Cisco	los Xe	2.6\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.1s\(.0\)	All	All	All
Operating System	Cisco	los Xe	3.1s\(.1\)	All	All	All
Operating System	Cisco	los Xe	3.1s\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.1s\(.3\)	All	All	All
Operating System	Cisco	los Xe	3.2s\(.0\)	All	All	All
Operating System	Cisco	los Xe	3.2s\(.1\)	All	All	All
Operating System	Cisco	los Xe	3.2s\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.3s\(.0\)	All	All	All
Operating System	Cisco	los Xe	3.3s\(.1\)	All	All	All
Operating System	Cisco	los Xe	3.3s\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.4s\(.0\)	All	All	All
Operating System	Cisco	los Xe	3.4s\(.1\)	All	All	All
Operating System	Cisco	los Xe	3.4s\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.4s\(.3\)	All	All	All
Operating System	Cisco	los Xe	3.4s\(.4\)	All	All	All
Operating System	Cisco	los Xe	3.4s\(.5\)	All	All	All
Operating System	Cisco	los Xe	3.4s\(.6\)	All	All	All
Operating System	Cisco	los Xe	3.5s\(.0\)	All	All	All
Operating System	Cisco	los Xe	3.5s\(.1\)	All	All	All
Operating System	Cisco	los Xe	3.5s\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.6s\(.0\)	All	All	All
Operating System	Cisco	los Xe	3.6s\(.1\)	All	All	All
Operating System	Cisco	los Xe	3.6s\(.2\)	All	All	All
Operating System	Cisco	los Xe	3.7s\(.0\)	All	All	All
Operating System	Cisco	los Xe	All	All	All	All
Operating System	Cisco	los Xe	All	All	All	All

Reference	Source	Link
Cisco IOS XE Software MPLS IP Fragmentation Denial of Service Vulnerability	BID	www.securityfocus.com
About Secunia Research Flexera	SECUNIA	secunia.com
Cisco Security Notice: Cisco IOS XE Crafted MPLS IP Fragmentation Denial of Service Vulnerability	CISCO	tools.cisco.com
Cisco IOS XE MPLS IP Fragmentation Bug Lets Remote Users Deny Service - SecurityTracker	SECTrack	www.securitytracker.com
Alert Details - Security Center - Cisco Systems	CONFIRM	tools.cisco.com
101423	OSVDB	osvdb.org
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

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

© [CVE.report](https://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](https://www.mitre.org) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve). This site includes MITRE data granted under the following [license](https://www.mitre.org/cve).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report