

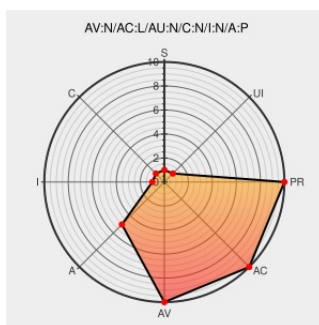


CVE-2015-4293

Published on: 07/30/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:06 PM UTC

CVE-2015-4293

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [ios Xe](#) from [Cisco](#) contain the following vulnerability:

The packet-reassembly implementation in Cisco IOS XE 3.13S and earlier allows remote attackers to cause a denial of service (CPU consumption or packet loss) via fragmented (1) IPv4 or (2) IPv6 packets that trigger ATTN-3-SYNC_TIMEOUT errors after reassembly failures, aka Bug ID CSCuo37957.

CVE-2015-4293 has been assigned by [cisco](#) psirt@cisco.com to track the vulnerability

CVSS2 Score: **5 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

NETWORK

LOW

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

NONE

PARTIAL

CVE References

Description

Tags

Link

Cisco IOS-XE Fragmented Packet Resource Consumption Vulnerability

[Vendor Advisory](#)
[tools.cisco.com](#)
[text/html](#)

[CISCO 20150729 Cisco IOS-XE Fragmented Packet Resource Consumption Vulnerability](#)

Cisco IOS-XE Packet Fragmentation Error Message Lets Remote Users Consume Excessive CPU Resources on the Target System - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTRAK 1033122](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE						
Known Affected Configurations (CPE V2.3)						
Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	ios Xe	2.1.0	All	All	All
Operating System	Cisco	ios Xe	2.1.1	All	All	All
Operating System	Cisco	ios Xe	2.1.2	All	All	All
Operating System	Cisco	ios Xe	2.2.1	All	All	All
Operating System	Cisco	ios Xe	2.2.2	All	All	All
Operating System	Cisco	ios Xe	2.2.3	All	All	All
Operating System	Cisco	ios Xe	2.3.0	All	All	All
Operating System	Cisco	ios Xe	2.3.0t	All	All	All
Operating System	Cisco	ios Xe	2.3.1t	All	All	All
Operating System	Cisco	ios Xe	2.3.2	All	All	All
Operating System	Cisco	ios Xe	2.4.0	All	All	All
Operating System	Cisco	ios Xe	2.4.1	All	All	All
Operating System	Cisco	ios Xe	2.5.0	All	All	All
Operating System	Cisco	ios Xe	2.5.1	All	All	All
Operating System	Cisco	ios Xe	2.5.2	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	3.10s.0	All	All	All
Operating System	Cisco	ios Xe	3.10s.0a	All	All	All
Operating	Cisco	ios Xe	3.10s.1	All	All	All

System						
Operating System	Cisco	los Xe	3.10s.2	All	All	All
Operating System	Cisco	los Xe	3.10s.3	All	All	All
Operating System	Cisco	los Xe	3.11s.0	All	All	All
Operating System	Cisco	los Xe	3.11s.1	All	All	All
Operating System	Cisco	los Xe	3.11s.2	All	All	All
Operating System	Cisco	los Xe	3.12s.0	All	All	All
Operating System	Cisco	los Xe	3.12s.1	All	All	All
Operating System	Cisco	los Xe	3.13s.0	All	All	All
Operating System	Cisco	los Xe	2.1.0	All	All	All
Operating System	Cisco	los Xe	2.1.1	All	All	All
Operating System	Cisco	los Xe	2.1.2	All	All	All
Operating System	Cisco	los Xe	2.2.1	All	All	All
Operating System	Cisco	los Xe	2.2.2	All	All	All
Operating System	Cisco	los Xe	2.2.3	All	All	All
Operating System	Cisco	los Xe	2.3.0	All	All	All
Operating System	Cisco	los Xe	2.3.0t	All	All	All
Operating System	Cisco	los Xe	2.3.1t	All	All	All
Operating System	Cisco	los Xe	2.3.2	All	All	All
Operating System	Cisco	los Xe	2.4.0	All	All	All
Operating System	Cisco	los Xe	2.4.1	All	All	All
Operating System	Cisco	los Xe	2.5.0	All	All	All
Operating System	Cisco	los Xe	2.5.1	All	All	All
Operating	Cisco	los Xe	2.5.2	All	All	All

System						
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	3.10s.0	All	All	All
Operating System	Cisco	Ios Xe	3.10s.0a	All	All	All
Operating System	Cisco	Ios Xe	3.10s.1	All	All	All
Operating System	Cisco	Ios Xe	3.10s.2	All	All	All
Operating System	Cisco	Ios Xe	3.10s.3	All	All	All
Operating System	Cisco	Ios Xe	3.11s.0	All	All	All
Operating System	Cisco	Ios Xe	3.11s.1	All	All	All
Operating System	Cisco	Ios Xe	3.11s.2	All	All	All
Operating System	Cisco	Ios Xe	3.12s.0	All	All	All
Operating System	Cisco	Ios Xe	3.12s.1	All	All	All
Operating System	Cisco	Ios Xe	3.13s.0	All	All	All
	cpe:2.3:o:cisco:ios_xe:2.1.0:*****:					
	cpe:2.3:o:cisco:ios_xe:2.1.1:*****:					
	cpe:2.3:o:cisco:ios_xe:2.1.2:*****:					
	cpe:2.3:o:cisco:ios_xe:2.2.1:*****:					
	cpe:2.3:o:cisco:ios_xe:2.2.2:*****:					
	cpe:2.3:o:cisco:ios_xe:2.2.3:*****:					
	cpe:2.3:o:cisco:ios_xe:2.3.0:*****:					
	cpe:2.3:o:cisco:ios_xe:2.3.0t:*****:					
	cpe:2.3:o:cisco:ios_xe:2.3.1t:*****:					
	cpe:2.3:o:cisco:ios_xe:2.3.2:*****:					

cpe:2.3:o:cisco:ios_xe:2.4.0:*****:
cpe:2.3:o:cisco:ios_xe:2.4.1:*****:
cpe:2.3:o:cisco:ios_xe:2.5.0:*****:
cpe:2.3:o:cisco:ios_xe:2.5.1:*****:
cpe:2.3:o:cisco:ios_xe:2.5.2:*****:
cpe:2.3:o:cisco:ios_xe:2.6.0:*****:
cpe:2.3:o:cisco:ios_xe:2.6.1:*****:
cpe:2.3:o:cisco:ios_xe:2.6.2:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.0:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.0a:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.1:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.2:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.3:*****:
cpe:2.3:o:cisco:ios_xe:3.11s.0:*****:
cpe:2.3:o:cisco:ios_xe:3.11s.1:*****:
cpe:2.3:o:cisco:ios_xe:3.11s.2:*****:
cpe:2.3:o:cisco:ios_xe:3.12s.0:*****:
cpe:2.3:o:cisco:ios_xe:3.12s.1:*****:
cpe:2.3:o:cisco:ios_xe:3.13s.0:*****:
cpe:2.3:o:cisco:ios_xe:2.1.0:*****:
cpe:2.3:o:cisco:ios_xe:2.1.1:*****:
cpe:2.3:o:cisco:ios_xe:2.1.2:*****:
cpe:2.3:o:cisco:ios_xe:2.2.1:*****:
cpe:2.3:o:cisco:ios_xe:2.2.2:*****:
cpe:2.3:o:cisco:ios_xe:2.2.3:*****:
cpe:2.3:o:cisco:ios_xe:2.3.0:*****:
cpe:2.3:o:cisco:ios_xe:2.3.0t:*****:
cpe:2.3:o:cisco:ios_xe:2.3.1t:*****:
cpe:2.3:o:cisco:ios_xe:2.3.2:*****:

cpe:2.3:o:cisco:ios_xe:2.4.0:*****:
cpe:2.3:o:cisco:ios_xe:2.4.1:*****:
cpe:2.3:o:cisco:ios_xe:2.5.0:*****:
cpe:2.3:o:cisco:ios_xe:2.5.1:*****:
cpe:2.3:o:cisco:ios_xe:2.5.2:*****:
cpe:2.3:o:cisco:ios_xe:2.6.0:*****:
cpe:2.3:o:cisco:ios_xe:2.6.1:*****:
cpe:2.3:o:cisco:ios_xe:2.6.2:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.0:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.0a:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.1:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.2:*****:
cpe:2.3:o:cisco:ios_xe:3.10s.3:*****:
cpe:2.3:o:cisco:ios_xe:3.11s.0:*****:
cpe:2.3:o:cisco:ios_xe:3.11s.1:*****:
cpe:2.3:o:cisco:ios_xe:3.11s.2:*****:
cpe:2.3:o:cisco:ios_xe:3.12s.0:*****:
cpe:2.3:o:cisco:ios_xe:3.12s.1:*****:
cpe:2.3:o:cisco:ios_xe:3.13s.0:*****:

No vendor comments have been submitted for this CVE

[← Previous ID](#)

[Next ID →](#)