



# CVE-2007-5651

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064\_img.jpg\)](#)

## Summary

<b>CVE</b>	CVE-2007-5651
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-10-23 21:47:00 UTC
<b>Updated</b>	2017-09-29 01:29:00 UTC
<b>Description</b>	Unspecified vulnerability in the Extensible Authentication Protocol (EAP) implementation in Cisco IOS 12.3 and 12.4 on Cis

## Risk And Classification

**Problem Types:** NVD-CWE-noinfo

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Catos	6.1	All	All	All
Operating System	Cisco	Catos	6.2	All	All	All
Operating System	Cisco	Catos	6.3	All	All	All
Operating System	Cisco	Catos	6.4	All	All	All
Operating System	Cisco	Catos	7.1	All	All	All
Operating System	Cisco	Catos	7.2	All	All	All
Operating System	Cisco	Catos	7.3	All	All	All
Operating System	Cisco	Catos	7.4	All	All	All
Operating System	Cisco	Catos	7.5	All	All	All
Operating System	Cisco	Catos	7.6	All	All	All
Operating System	Cisco	Catos	8.1	All	All	All
Operating System	Cisco	Catos	8.2	All	All	All
Operating System	Cisco	Catos	8.3	All	All	All
Operating System	Cisco	Catos	8.4	All	All	All
Operating System	Cisco	Catos	8.5	All	All	All
Operating System	Cisco	Catos	6.1	All	All	All
Operating System	Cisco	Catos	6.2	All	All	All

Operating System	Cisco	Catos	6.3	All	All	All
Operating System	Cisco	Catos	6.4	All	All	All
Operating System	Cisco	Catos	7.1	All	All	All
Operating System	Cisco	Catos	7.2	All	All	All
Operating System	Cisco	Catos	7.3	All	All	All
Operating System	Cisco	Catos	7.4	All	All	All
Operating System	Cisco	Catos	7.5	All	All	All
Operating System	Cisco	Catos	7.6	All	All	All
Operating System	Cisco	Catos	8.1	All	All	All
Operating System	Cisco	Catos	8.2	All	All	All
Operating System	Cisco	Catos	8.3	All	All	All
Operating System	Cisco	Catos	8.4	All	All	All
Operating System	Cisco	Catos	8.5	All	All	All
Operating System	Cisco	ios	12.1	All	All	All
Operating System	Cisco	ios	12.2	All	All	All
Operating System	Cisco	ios	12.3ja	All	All	All
Operating System	Cisco	ios	12.3jea	All	All	All
Operating System	Cisco	ios	12.3jeb	All	All	All
Operating System	Cisco	ios	12.3jec	All	All	All
Operating System	Cisco	ios	12.4ja	All	All	All
Operating System	Cisco	ios	12.1	All	All	All
Operating System	Cisco	ios	12.2	All	All	All
Operating System	Cisco	ios	12.3ja	All	All	All
Operating System	Cisco	ios	12.3jea	All	All	All
Operating System	Cisco	ios	12.3jeb	All	All	All
Operating System	Cisco	ios	12.3jec	All	All	All
Operating System	Cisco	ios	12.4ja	All	All	All

## References

Reference	Source	L
Repository / Oval Repository	OVAL	o
SecurityTracker.com Archives - Cisco IOS Extensible Authentication Protocol (EAP) Bug Lets Remote Users Deny Service	SECTRACK	w
Cisco Security Response: Extensible Authentication Protocol Vulnerability [Products & Services] - Cisco Systems	CISCO	w
Cisco Multiple Products Extensible Authentication Protocol Denial of Service Vulnerability	BID	w
IBM X-Force Exchange	XF	e
W... ..	W... ..	

Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="#">w</a>
Cisco Products EAP Denial of Service Vulnerability - Advisories - Secunia	SECUNIA	<a href="#">s</a>
CVE Program record	CVE.ORG	<a href="#">w</a>
NVD vulnerability detail	NVD	<a href="#">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](#)