



# CVE-2007-4012

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

## Summary

<b>CVE</b>	CVE-2007-4012
<b>State</b>	PUBLIC
<b>Assigner</b>	cve@mitre.org
<b>Source Priority</b>	CVE Program / NVD first with legacy fallback
<b>Published</b>	2007-07-26 00:30:00 UTC
<b>Updated</b>	2018-10-30 16:25:00 UTC
<b>Description</b>	Cisco 4100 and 4400, Airespace 4000, and Catalyst 6500 and 3750 Wireless LAN Controller (WLC) software 4.1 before 4.1

## Risk And Classification

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

## NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	4100 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	4100 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	4400 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	4400 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	Airespace 4000 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	Airespace 4000 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	Catalyst 3750	All	All	All	All
Hardware	Cisco	Catalyst 3750	All	All	All	All
Hardware	Cisco	Catalyst 6500	All	All	All	All
Hardware	Cisco	Catalyst 6500	All	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	3.2	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	3.2.116.21	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	4.0	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	4.0.155.0	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	4.1	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	3.2	All	All	All
Operating System	Cisco	Wireless Lan Controller Software	3.2.116.21	All	All	All

Operating System	Cisco	<a href="#">Wireless Lan Controller Software</a>	4.0	All	All	All
Operating System	Cisco	<a href="#">Wireless Lan Controller Software</a>	4.0.155.0	All	All	All
Operating System	Cisco	<a href="#">Wireless Lan Controller Software</a>	4.1	All	All	All

## References

Reference	Source	Link
Wireless ARP Storm Vulnerabilities - Cisco Systems	CISCO	<a href="http://www.cisco.com">www.cisco.com</a>
Cisco Multiple Products Wireless ARP Requests Denial of Service - Advisories - Secunia	SECUNIA	<a href="http://secunia.com">secunia.com</a>
Cisco Wireless LAN Control ARP Storm Multiple Denial Of Service Vulnerabilities	BID	<a href="http://www.securityfocus.com">www.securityfocus.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
IBM X-Force Exchange	XF	<a href="http://exchange.xforce.ibmcloud.com">exchange.xforce.ibmcloud.com</a>
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN	<a href="http://www.vupen.com">www.vupen.com</a>
Cisco Wireless LAN Controller ARP Processing Lets Remote Users Deny Service - SecurityTracker	SECTRACK	<a href="http://www.securitytracker.com">www.securitytracker.com</a>
CVE Program record	CVE.ORG	<a href="http://www.cve.org">www.cve.org</a>
NVD vulnerability detail	NVD	<a href="http://nvd.nist.gov">nvd.nist.gov</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](http://status.cve.report)