



CVE-2007-2038

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

Summary

CVE	CVE-2007-2038
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2007-04-16 21:19:00 UTC
Updated	2017-07-29 01:31:00 UTC
Description	The Network Processing Unit (NPU) in the Cisco Wireless LAN Controller (WLC) before 3.2.193.5, 4.0.x before 4.0.206.0, and 4.2.x before 4.2.208.0 contains a buffer overflow vulnerability that could allow an attacker to execute arbitrary code or cause a denial of service (DoS) on the affected device. The vulnerability is located in the NPU's handling of the configuration file. The vulnerability is caused by a buffer overflow in the NPU's handling of the configuration file. The vulnerability is caused by a buffer overflow in the NPU's handling of the configuration file.

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	2000 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	2000 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	2100 Wireless Lan Controller	All	All	All	All
Hardware	Cisco	2100 Wireless Lan Controller	All	All	All	All
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

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VUPEN
SecurityTracker.com Archives - Cisco Wireless LAN Controller Lets Remote Users Modify the Configuration and Deny Service	SECTRAK
34136	OSVDB
IBM X-Force Exchange	XF
Cisco - Networking, Cloud, and Cybersecurity Solutions	CISCO
Cisco Wireless Lan Controller Multiple Remote Vulnerabilities	BID

CVE Program record	CVE.ORG
NVD vulnerability detail	NVD
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](#).

Free CVE JSON API [cve.report/api](#)

CVE.report and Source URL Uptime Status [status.cve.report](#)