



CVE-2008-4391

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

Summary

CVE	CVE-2008-4391
State	PUBLIC
Assigner	cert@cert.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2008-12-09 00:30:00 UTC
Updated	2009-08-20 05:21:00 UTC
Description	Stack-based buffer overflow in the SetSource method in the NetCamPlayerWeb11gv2 ActiveX control in NetCamPlayerWeb11gv2.ocx in Linksys WVC54GC routers.

Risk And Classification

Problem Types: CWE-119

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Cisco	Wvc54gc	1.15	All	All	All
Hardware	Cisco	Wvc54gc	1.15	All	All	All
Hardware	Cisco	Wvc54gc	All	All	All	All

References

Reference	Source	Link	Tags
Linksys WVC54GC 'NetCamPlayerWeb11gv2.ocx' ActiveX Control Buffer Overflow Vulnerability	BID	www.securityfocus.com	
Linksys WVC54GC Information Disclosure and ActiveX Control Buffer Overflow - Secunia.com	SECUNIA	secunia.com	
VU#639345 - Linksys WVC54GC NetCamPlayerWeb11gv2 ActiveX control stack buffer overflow	CERT-VN	www.kb.cert.org	Partial
Linksys (A division of Cisco Systems) Information for VU#639345	CONFIRM	www.kb.cert.org	US
CVE Program record	CVE.ORG	www.cve.org	Canonical
NVD vulnerability detail	NVD	nvd.nist.gov	Canonical

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](#)