



CVE-2004-1790

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2004-1790
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2004-12-31 05:00:00 UTC
Updated	2017-07-11 01:31:00 UTC
Description	Cross-site scripting (XSS) vulnerability in the web management interface in Edimax AR-6004 ADSL Routers allows remote

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	Edimax	Full Rate Adsl Router	ar_6004	All	All	All
Hardware	Edimax	Full Rate Adsl Router	ar_6004	All	All	All

References

Reference	Source	Link
Secunia - Advisories - EDIMAX AR-6004 Broadband Router Cross-Site Scripting Vulnerability	SECUNIA	secunia.c
SecurityTracker.com Archives - Edimax AR-6004 Router Input Validation Flaw Permits Cross-Site Scripting Attacks	SECTRACK	securitytr
3435	OSVDB	www.osv
Edimax AR-6004 ADSL Router Management Interface Cross-Site Scripting Vulnerability	BID	www.sec
SecurityFocus	BUGTRAQ	www.sec
IBM X-Force Exchange	XF	exchange
CVE Program record	CVE.ORG	www.cve
NVD vulnerability detail	NVD	nvd.nist.c

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](#)