



CVE-2014-3761

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

Summary

CVE	CVE-2014-3761
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-16 14:55:00 UTC
Updated	2023-04-26 19:27:00 UTC
Description	Cross-site scripting (XSS) vulnerability in D-Link DAP 1150 with firmware 1.2.94 allows remote attackers to inject arbitrary v

Risk And Classification

Problem Types: CWE-79

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware	D-link	Dap 1150	-	All	All	All
Hardware	D-link	Dap 1150	-	All	All	All
Operating System	D-link	Dap 1150 Firmware	1.2.94	All	All	All
Operating System	D-link	Dap 1150 Firmware	1.2.94	All	All	All
Hardware	Dlink	Dap 1150	-	All	All	All
Operating System	Dlink	Dap 1150 Firmware	1.2.94	All	All	All

References

Reference	Source	Link	Tags
CSRF, AoF та XSS уразливості в D-Link DAP 1150 - Websecurity - Веб безпека	MISC	websecurity.com.ua	Exploit
Full Disclosure: CSRF, AoF and XSS vulnerabilities in D-Link DAP 1150	FULLDISC	seclists.org	Exploit
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#)