



CVE-2015-6428

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

Summary

CVE	CVE-2015-6428
State	PUBLIC
Assigner	psirt@cisco.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2015-12-18 11:59:00 UTC
Updated	2016-12-07 18:20:00 UTC
Description	Cisco DPQ3925 devices with EDVA r1 Base allow remote attackers to obtain sensitive information via a crafted HTTP requ

Risk And Classification

Problem Types: CWE-200

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Up
Operating System	Cisco	Dpq3925 8x4 Docsis 3.0 Wireless Residential Gateway With Embedded Digital Voice Adapter	r1_base	All
Operating System	Cisco	Dpq3925 8x4 Docsis 3.0 Wireless Residential Gateway With Embedded Digital Voice Adapter	r1_base	All

References

Reference

- Cisco Wireless Residential Gateway CVE-2015-6428 Information Disclosure Vulnerability
- Cisco DPQ3925 Wireless Residential Gateway Input Validation Flaw in HTTP Server Lets Remote Users Obtain Potentially Sensitive Informat
- Cisco Model DPQ3925 Wireless Residential Gateway Information Disclosure Vulnerability
- CVE Program record
- NVD vulnerability detail

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

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](#)