

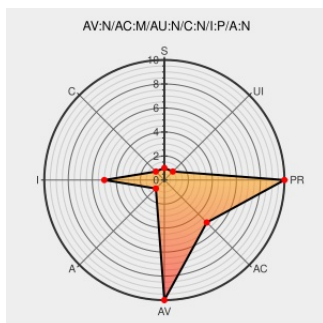


CVE-2015-6402

Published on: 12/13/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:17 PM UTC

CVE-2015-6402

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Epc3928 Docsis 3.0 8x4 Wireless Residential Gateway With Embedded Digital Voice Adapter](#) from [Cisco](#) contain the following vulnerability:

Cross-site scripting (XSS) vulnerability in the management interface on Cisco EPC3928 devices with EDVA 5.5.10, 5.5.11, and 5.7.1 allows remote attackers to inject arbitrary web script or HTML via an unspecified value, aka Bug ID CSCux24935.

CVE-2015-6402 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability

CVSS2 Score: **4.3 - MEDIUM**

Access Vector

Access Complexity

Authentication

NETWORK

MEDIUM

NONE

Confidentiality Impact

Integrity Impact

Availability Impact

NONE

PARTIAL

NONE

CVE References

Description

Tags

Link

Cisco Wireless Residential Gateway Stored Cross-Site Scripting Vulnerability

[Vendor Advisory](#)
[tools.cisco.com](#)
[text/html](#)

[CISCO 20151208 Cisco Wireless Residential Gateway Stored Cross-Site Scripting Vulnerability](#)

Cisco Wireless Residential Gateway EPC3928 Input Validation Flaw Lets Remote Conduct Cross-Site Scripting Attacks - SecurityTracker

[www.securitytracker.com](#)
[text/html](#)

[SECTrack 1034346](#)

Cisco EPC 3928 - Multiple Vulnerabilities - ASP webapps Exploit

[www.exploit-db.com](#)
[Proof of Concept](#)
[text/html](#)

[EXPLOIT-DB 39904](#)

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Cisco	Epc3928 Docsis 3.0 8x4 Wireless Residential Gateway With Embedded Digital Voice Adapter	5.5.10	All	All	All
Operating System	Cisco	Epc3928 Docsis 3.0 8x4 Wireless Residential Gateway With Embedded Digital Voice Adapter	5.5.11	All	All	All
Operating System	Cisco	Epc3928 Docsis 3.0 8x4 Wireless Residential Gateway With Embedded Digital Voice Adapter	5.7.1	All	All	All
Operating System	Cisco	Epc3928 Docsis 3.0 8x4 Wireless Residential Gateway With Embedded Digital Voice Adapter	5.5.10	All	All	All
Operating System	Cisco	Epc3928 Docsis 3.0 8x4 Wireless Residential Gateway With Embedded Digital Voice Adapter	5.5.11	All	All	All
Operating System	Cisco	Epc3928 Docsis 3.0 8x4 Wireless Residential Gateway With Embedded Digital Voice Adapter	5.7.1	All	All	All
cpe:2.3:o:cisco:epc3928_docsis_3.0_8x4_wireless_residential_gateway_with_embedded_digital_voice_adapter:5.5.10:*****:						
cpe:2.3:o:cisco:epc3928_docsis_3.0_8x4_wireless_residential_gateway_with_embedded_digital_voice_adapter:5.5.11:*****:						
cpe:2.3:o:cisco:epc3928_docsis_3.0_8x4_wireless_residential_gateway_with_embedded_digital_voice_adapter:5.7.1:*****:						
cpe:2.3:o:cisco:epc3928_docsis_3.0_8x4_wireless_residential_gateway_with_embedded_digital_voice_adapter:5.5.10:*****:						
cpe:2.3:o:cisco:epc3928_docsis_3.0_8x4_wireless_residential_gateway_with_embedded_digital_voice_adapter:5.5.11:*****:						
cpe:2.3:o:cisco:epc3928_docsis_3.0_8x4_wireless_residential_gateway_with_embedded_digital_voice_adapter:5.7.1:*****:						

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→