

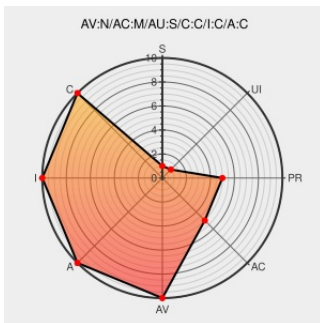


CVE-2015-8227

Published on: 11/24/2015 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:14 PM UTC

CVE-2015-8227

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

Certain versions of [Vp9660](#) from [Huawei](#) contain the following vulnerability:

The built-in web server in Huawei VP9660 multi-point control unit with software before V200R001C30SPC700 allows remote administrators to obtain sensitive information or cause a denial of service via a crafted message.

CVE-2015-8227 has been assigned by [M](#) cve@mitre.org to track the vulnerability

CVSS2 Score: **8.5 - HIGH**

Access
Vector

NETWORK

Access
Complexity

MEDIUM

Authentication

SINGLE

Confidentiality
Impact

COMPLETE

Integrity
Impact

COMPLETE

Availability
Impact

COMPLETE

CVE References

Description

Tags

Link

Security Advisory - Input Validation Vulnerability in Huawei VP9660 Products

[Vendor Advisory](#)

[web.archive.org](#)

[text/html](#)

[Inactive Link](#)

[Not Archived](#)

CONFIRM

www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-461216.htm

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 comment@cve.report.

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Known Affected Configurations (CPE V2.0)

Type	Vendor	Product	Version	Update	Edition	Language
Hardware 🇨🇳 ↗️	Huawei	Vp9660	-	All	All	All
Hardware 🇨🇳 ↗️	Huawei	Vp9660	-	All	All	All
Operating System	Huawei	Vp 9660 Firmware	v200r001c01	All	All	All
Operating System	Huawei	Vp 9660 Firmware	v200r001c02	All	All	All
Operating System	Huawei	Vp 9660 Firmware	v200r001c01	All	All	All
Operating System	Huawei	Vp 9660 Firmware	v200r001c02	All	All	All
Operating System	Huawei	Vp 9660 Firmware	All	All	All	All
cpe:2.3:h:huawei:vp9660:-:*:*:*:*:*:						
cpe:2.3:h:huawei:vp9660:-:*:*:*:*:*:						
cpe:2.3:o:huawei:vp_9660_firmware:v200r001c01:*:*:*:*:*:						
cpe:2.3:o:huawei:vp_9660_firmware:v200r001c02:*:*:*:*:*:						
cpe:2.3:o:huawei:vp_9660_firmware:v200r001c01:*:*:*:*:*:						
cpe:2.3:o:huawei:vp_9660_firmware:v200r001c02:*:*:*:*:*:						
cpe:2.3:o:huawei:vp_9660_firmware:*:*:*:*:*:						

No vendor comments have been submitted for this CVE

[← Previous ID](#)

Next ID→

© CVE.report 2023 |

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