



CVE-2013-1131

Published on: 02/13/2013 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:28:31 PM UTC

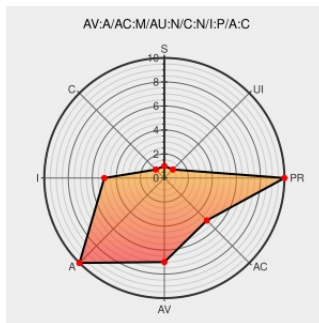
CVE-2013-1131

Source: Mitre

Source: NIST

CVE.ORG

Print: PDF



Certain versions of [Small Business Wireless Access Ppoints](#) from [Cisco](#) contain the following vulnerability:

Cisco Small Business Wireless Access Points WAP200, WAP2000, WAP200E, and WET200 allow remote attackers to cause a denial of service or possibly have unspecified other impact via a crafted SSID that is not properly handled during a site survey, aka Bug IDs CSCua86182, CSCua91196, CSCud36155, and CSCua86190.

CVE-2013-1131 has been assigned by [Cisco](#) psirt@cisco.com to track the vulnerability

CVSS2 Score: **6.4 - MEDIUM**

Access
Vector

Access
Complexity

Authentication

ADJACENT_NETWORK

MEDIUM

NONE

Confidentiality
Impact

Integrity
Impact

Availability
Impact

NONE

PARTIAL

COMPLETE

CVE References

Description

Tags

Link

Cisco Small Business Wireless Access Points SSID Validation Vulnerability

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

[CISCO 20130213 Cisco Small Business Wireless Access Points SSID Validation Vulnerability](#)

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

