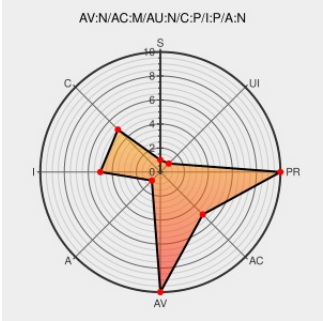
CVE-2011-5053

Published on: 01/06/2012 12:00:00 AM UTC

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

CVE-2011-5053

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Wifi Protected Setup Protocol from Wi-fi contain the following vulnerability:

The Wi-Fi Protected Setup (WPS) protocol, when the "external registrar" authentication method is used, does not properly inform clients about failed PIN authentication, which makes it easier for remote attackers to discover the PIN value, and consequently discover the Wi-Fi network password or reconfigure an access point, by reading EAP-NACK messages.

CVE-2011-5053 has been assigned by cert@cert.org to track the vulnerability

CVSS2 Score: 5.8 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	PARTIAL	NONE

CVE References

Description	Tags	Link
VU#723755 - WiFi Protected Setup (WPS) PIN brute force vulnerability	US Government Resource, www.kb.cert.org, text/html	CERT-VN VU#723755
Wi-Fi Protected Setup PIN brute force vulnerability « .braindump – RE and stuff	sviehb.wordpress.com, text/html	MISC sviehb.wordpress.com/2011/12/27/wi-fi-protected-setup-pin-brute-force-vulnerability/
reaver-wps - Brute force attack against Wifi Protected Setup - Google Project Hosting	code.google.com, text/html	MISC code.google.com/p/reaver-wps/
US-CERT Technical Cyber Security Alert TA12-006A -- Wi-Fi Protected Setup (WPS) Vulnerable to Brute-Force Attack	US Government Resource, www.us-cert.gov, text/xml	CERT TA12-006A

Wi-Fi Protected Setup PIN Brute Force Vulnerability	tools.cisco.com text/html	CISCO 20120111 Wi-Fi Protected Setup PIN Brute Force Vulnerability
	sviehb.files.wordpress.com application/pdf	MISC sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf

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)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Wi-fi	Wifi Protected Setup Protocol	All	All	All	All
Application	Wi-fi	Wifi Protected Setup Protocol	All	All	All	All

cpe:2.3:a:wi-fi:wifi_protected_setup_protocol:*:*:*:*:*:*:*:*:

cpe:2.3:a:wi-fi:wifi_protected_setup_protocol:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→