



CVE-2005-3253

- MITRE
- NVD
- CVE.ORG
- JSON API
- Print: PDF

Summary

CVE	CVE-2005-3253
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2005-12-16 11:03:00 UTC
Updated	2025-04-03 01:03:51 UTC
Description	Wireless Access Points (AP) for (1) Avaya AP-3 through AP-6 2.5 to 2.5.4, and AP-7/AP-8 2.5 and other versions before 3.

Risk And Classification

Primary CVSS: v2.0 7.5 from nvd@nist.gov

AV:N/AC:L/Au:N/C:P/I:P/A:P

Problem Types: NVD-CWE-Other | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

None

Confidentiality

Partial

Integrity

Partial

Availability

Partial

AV:N/AC:L/Au:N/C:P/I:P/A:P

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Avaya	Wireless Ap-3	2.5	All	All	All

Application	Avaya	Wireless Ap-3	2.5.4	All	All	All
Application	Avaya	Wireless Ap-4	2.5	All	All	All
Application	Avaya	Wireless Ap-4	2.5.4	All	All	All
Application	Avaya	Wireless Ap-5	2.5	All	All	All
Application	Avaya	Wireless Ap-5	2.5.4	All	All	All
Application	Avaya	Wireless Ap-6	2.5	All	All	All
Application	Avaya	Wireless Ap-6	2.5.4	All	All	All
Application	Avaya	Wireless Ap-7	2.5	All	All	All
Application	Avaya	Wireless Ap-8	2.5	All	All	All
Hardware	Proxim	Ap-2000	2.5.4	All	All	All
Hardware	Proxim	Ap-4000	2.4.12	All	All	All
Hardware	Proxim	Ap-4000	3.0	All	All	All
Hardware	Proxim	Ap-600	2.5.4	All	All	All
Hardware	Proxim	Ap-700	2.4.12	All	All	All
Hardware	Proxim	Ap-700	3.0	All	All	All

Vendor Declared Affected Products						
Source	Vendor	Product	Version	Platforms		
CNA	Na	N/a	affected n/a	Not specified		

References	
Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	af854a3a-2127-422b-91ae-364da2661108
support.avaya.com/elmodocs2/security/ASA-2005-233.pdf	af854a3a-2127-422b-91ae-364da2661108
Proxim Wireless Access Points Static WEP Key Authentication Bypass - Advisories - Secunia	af854a3a-2127-422b-91ae-364da2661108
Secunia - Advisories - Avaya Wireless Access Points Static WEP Key Authentication Bypass	af854a3a-2127-422b-91ae-364da2661108
keygen.proxim.com/support/cs/Documents/802.1x_vulnerability.pdf	af854a3a-2127-422b-91ae-364da2661108
www.osvdb.org/22091	af854a3a-2127-422b-91ae-364da2661108
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

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](#).

Free CVE JSON API cve.report/api

CVE.report and Source URL Uptime Status status.cve.report