



CVE-2013-6766

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

Summary

CVE	CVE-2013-6766
State	PUBLISHED
Assigner	mitre
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-05-19 14:55:09 UTC
Updated	2026-05-06 22:30:45 UTC
Description	OpenVAS Administrator 1.2 before 1.2.2 and 1.3 before 1.3.2 allows remote attackers to bypass the OAP authentication re

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: CWE-287 | 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	Openvas	Openvas Administrator	1.2	rc1	All	All

Application	Openvas	Openvas Administrator	1.2.0	All	All	All
Application	Openvas	Openvas Administrator	1.2.1	All	All	All
Application	Openvas	Openvas Administrator	1.3	beta1	All	All
Application	Openvas	Openvas Administrator	1.3	rc1	All	All
Application	Openvas	Openvas Administrator	1.3.0	All	All	All
Application	Openvas	Openvas Administrator	1.3.1	All	All	All

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

References		
Reference	Source	Link
oss-security - CVE-2013-6765 CVE-2013-6766 for OpenVAS 4.0.4/1.3.2/etc.	af854a3a-2127-422b-91ae-364da2661108	www.openwall.co
OpenVAS - OpenVAS	af854a3a-2127-422b-91ae-364da2661108	www.openvas.org
[Openvas-announce] Security Releases for OpenVAS-5 and OpenVAS-6	af854a3a-2127-422b-91ae-364da2661108	lists.wald.intevati
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.