



CVE-2014-0132

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2014-0132
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2014-03-18 17:02:53 UTC
Updated	2026-05-06 22:30:45 UTC
Description	The SASL authentication functionality in 389 Directory Server before 1.2.11.26 allows remote authenticated users to connect to the server and perform administrative tasks.

Risk And Classification

Primary CVSS: v2.0 6.5 from nvd@nist.gov

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

Problem Types: CWE-287 | n/a

CVSS v2.0 Breakdown

Access Vector

Network

Access Complexity

Low

Authentication

Single

Confidentiality

Partial

Integrity

Partial

Availability

Partial

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	389 Directory Server	1.2.11.1	All	All	All

Application	Fedoraproject	389 Directory Server	1.2.11.10	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.11	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.12	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.13	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.14	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.15	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.17	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.19	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.20	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.21	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.22	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.23	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.5	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.6	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.8	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.11.9	All	All	All
Application	Fedoraproject	389 Directory Server	All	All	All	All

Vendor Declared Affected Products

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

References

Reference	Source
Red Hat Customer Portal	af854a3a-2127-422f-b011-644c607998b4
Infrastructure/Fedorahosted-retirement - Fedora Project Wiki	af854a3a-2127-422f-b011-644c607998b4
Security Advisory SA57427 - 389 Directory Server SASL/GSSAPI Security Bypass Security Issue - Secunia	af854a3a-2127-422f-b011-644c607998b4
Security Advisory SA57412 - Red Hat update for 389-ds-base - Secunia	af854a3a-2127-422f-b011-644c607998b4
Issue #47739: directory server is insecurely misinterpreting authzid on a SASL/GSSAPI bind - 389-ds-base - Pagure.io	af854a3a-2127-422f-b011-644c607998b4
Red Hat Customer Portal	MITRE
access.redhat.com CVE-2014-0132	MITRE
1074845 – (CVE-2014-0132) CVE-2014-0132 389-ds: flaw in parsing authzid can lead to privilege escalation	MITRE
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.

© [CVE.report](#) 2026 |

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](#)