



CVE-2011-0022

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

Summary

CVE	CVE-2011-0022
State	PUBLISHED
Assigner	redhat
Source Priority	CVE Program / NVD first with legacy fallback
Published	2011-02-23 19:00:01 UTC
Updated	2026-04-29 01:13:23 UTC
Description	The setup scripts in 389 Directory Server 1.2.x (aka Red Hat Directory Server 8.2.x), when multiple unprivileged instances are running, can cause a denial of service (DoS) by consuming excessive memory and CPU resources. This issue affects 389 Directory Server versions 1.2.0 through 1.2.10, and Red Hat Directory Server versions 8.2.0 through 8.2.10. The issue was discovered by [REDACTED].

Risk And Classification

Primary CVSS: v2.0 4.7 from nvd@nist.gov

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

Problem Types: CWE-399 | n/a

CVSS v2.0 Breakdown

Access Vector

Local

Access Complexity

Medium

Authentication

None

Confidentiality

None

Integrity

None

Availability

Complete

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

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Fedoraproject	389 Directory Server	1.2.1	All	All	All

Application	Fedoraproject	389 Directory Server	1.2.2	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.3	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.5	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.5	rc1	All	All
Application	Fedoraproject	389 Directory Server	1.2.5	rc2	All	All
Application	Fedoraproject	389 Directory Server	1.2.5	rc3	All	All
Application	Fedoraproject	389 Directory Server	1.2.5	rc4	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	a2	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	a3	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	a4	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	rc1	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	rc2	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	rc3	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	rc6	All	All
Application	Fedoraproject	389 Directory Server	1.2.6	rc7	All	All
Application	Fedoraproject	389 Directory Server	1.2.6.1	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.7	alpha3	All	All
Application	Fedoraproject	389 Directory Server	1.2.7.5	All	All	All
Application	Fedoraproject	389 Directory Server	1.2.8	alpha1	All	All
Application	Fedoraproject	389 Directory Server	1.2.8	alpha2	All	All
Application	Redhat	Directory Server	8.2	All	All	All
Application	Redhat	Directory Server	8.2.3	All	All	All

Vendor Declared Affected Products

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

References

Reference	Sou
Red Hat Directory Server Bugs Let Local Users Gain Elevated Privileges and Remote and Local Users Deny Service - SecurityTracker	af85
671199 – (CVE-2011-0022) CVE-2011-0022 Directory Server: insecure pid file directory permissions	af85
Red Hat Directory Server Multiple Security Vulnerabilities	af85
rhn.redhat.com Red Hat Support	af85
CVE Program record	CVE
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](#)