CVE-2013-0312

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

Summary

CVE	CVE-2013-0312
State	PUBLIC
Assigner	secalert@redhat.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2013-03-13 20:55:00 UTC
Updated	2013-03-19 04:00:00 UTC
Description	389 Directory Server before 1.3.0.4 allows remote attackers to cause a denial of service (crash) via a zero length LDAP cor

Risk And Classification

Problem Types: CWE-189

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Sou
directory.fedoraproject.org/wiki/Releases/1.3.0.4	CON
Security Advisory SA52279 - 389 Directory Server LDAP Control Data Handling Denial of Service Vulnerability - Secunia	SEC
389 Directory Server CVE-2013-0312 Remote Denial of Service Vulnerability	BID
Security Advisory SA52568 - Red Hat update for 389-ds-base - Secunia	SEC
Red Hat Customer Portal	RED
Issue #571: server does not accept 0 length LDAP Control sequence - 389-ds-base - Pagure.io	MIS
912964 – (CVE-2013-0312) CVE-2013-0312 389-ds: unauthenticated denial of service vulnerability in handling of LDAPv3 control data	MIS
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.

Free CVE JSON API cve.report/api

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