



CVE-2009-0895

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

Summary

CVE	CVE-2009-0895
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2009-12-03 17:30:00 UTC
Updated	2017-08-17 01:30:00 UTC
Description	Integer overflow in Novell eDirectory 8.7.3.x before 8.7.3.10 ftf2 and 8.8.x before 8.8.5.2 allows remote attackers to execute

Risk And Classification

Problem Types: CWE-189

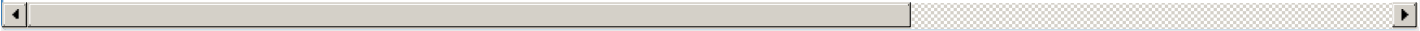
NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Edirectory	8.7.3	All	All	All
Application	Novell	Edirectory	8.7.3	sp10	All	All
Application	Novell	Edirectory	8.7.3	sp10	ftf1	All
Application	Novell	Edirectory	8.7.3	sp10_b	All	All
Application	Novell	Edirectory	8.7.3	sp3	All	All
Application	Novell	Edirectory	8.7.3	sp3	ftf1	All
Application	Novell	Edirectory	8.7.3	sp4	All	All
Application	Novell	Edirectory	8.7.3	sp4	ftf1	All
Application	Novell	Edirectory	8.7.3	sp5	All	All
Application	Novell	Edirectory	8.7.3	sp5	ftf1	All
Application	Novell	Edirectory	8.7.3.10	All	All	All
Application	Novell	Edirectory	8.7.3.8	All	All	All
Application	Novell	Edirectory	8.7.3.9	All	All	All
Application	Novell	Edirectory	8.8	All	All	All
Application	Novell	Edirectory	8.8	sp1	All	All
Application	Novell	Edirectory	8.8	sp2	All	All
Application	Novell	Edirectory	8.8	sp3	ftf3	All

Application	Novell	Edirectory	8.8	sp4	All	All
Application	Novell	Edirectory	8.8.1	All	All	All
Application	Novell	Edirectory	8.8.2	All	All	All
Application	Novell	Edirectory	8.8.2	All	ftf1	All
Application	Novell	Edirectory	8.8.5	All	ftf1	All
Application	Novell	Edirectory	8.7.3	All	All	All
Application	Novell	Edirectory	8.7.3	sp10	All	All
Application	Novell	Edirectory	8.7.3	sp10	ftf1	All
Application	Novell	Edirectory	8.7.3	sp10_b	All	All
Application	Novell	Edirectory	8.7.3	sp3	All	All
Application	Novell	Edirectory	8.7.3	sp3	ftf1	All
Application	Novell	Edirectory	8.7.3	sp4	All	All
Application	Novell	Edirectory	8.7.3	sp4	ftf1	All
Application	Novell	Edirectory	8.7.3	sp5	All	All
Application	Novell	Edirectory	8.7.3	sp5	ftf1	All
Application	Novell	Edirectory	8.7.3.10	All	All	All
Application	Novell	Edirectory	8.7.3.8	All	All	All
Application	Novell	Edirectory	8.7.3.9	All	All	All
Application	Novell	Edirectory	8.8	All	All	All
Application	Novell	Edirectory	8.8	sp1	All	All
Application	Novell	Edirectory	8.8	sp2	All	All
Application	Novell	Edirectory	8.8	sp3	ftf3	All
Application	Novell	Edirectory	8.8	sp4	All	All
Application	Novell	Edirectory	8.8.1	All	All	All
Application	Novell	Edirectory	8.8.2	All	All	All
Application	Novell	Edirectory	8.8.2	All	ftf1	All
Application	Novell	Edirectory	8.8.5	All	ftf1	All

References						
Reference						Sou
Novell eDirectory NDS Verb 0x1 Request Integer Overflow Vulnerability - Secunia Advisories - Vulnerability Information - Secunia.com						SEC
Support Security Vulnerability: Novell eDirectory Heap-based Buffer Overflow						COM
Access Denied						MIS
Novell eDirectory Heap-based buffer overflow						ISS
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH						VUF
Avec D... ..						MIS

Access Denied	MIS
Novell eDirectory 'NDS Verb 0x1' Request Heap Based Buffer Overflow Vulnerability	BID
IBM X-Force Exchange	XF
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](#)