



CVE-2006-4177

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

Summary

CVE	CVE-2006-4177
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-10-24 20:07:00 UTC
Updated	2017-07-20 01:32:00 UTC
Description	Heap-based buffer overflow in the NCP engine in Novell eDirectory before 8.8.1 FTF1 allows remote attackers to execute a

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Novell	Edirectory	8.8	All	All	All
Application	Novell	Edirectory	8.8	All	All	All
Application	Novell	Edirectory	All	All	All	All

References

Reference
IBM X-Force Exchange
support.novell.com/cgi-bin/search/searchtid.cgi
Public Advisory: 10.21.06 // iDefense Labs
Novell eDirectory NCP Over IP and evtFilteredMonitorEventsRequest() Overflows Let Remote Users Execute Arbitrary Code - SecurityTracke
Novell eDirectory Multiple Vulnerabilities - Advisories - Secunia
Novell eDirectory NCP Packet Processing Remote Heap Overflow Vulnerability
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH
CVE Program record
NVD vulnerability detail

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](#)