



CVE-2006-4803

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

Summary

CVE	CVE-2006-4803
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2006-09-14 22:07:00 UTC
Updated	2018-09-27 21:30:00 UTC
Description	The Fan-Out Linux and UNIX receiver scripts in Novell Identity Manager (IDM) 3.0.1 allows local users to execute arbitrary

Risk And Classification

Problem Types: NVD-CWE-Other

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Netiq	Identity Manager	3.0.1	All	All	All
Application	Netiq	Identity Manager	3.0.1	All	All	All

References

Reference	Source
Webmail : Solution de messagerie professionnelle - OVHcloud- OVH	VULNERABILITY
Security Advisory SA21888 - Novell Identity Manager Shell Scripts Command Injection - Secunia	SECURITY
SecurityTracker.com Archives - Novell Identity Manager Environment Variable Validation Bug Lets Local Users Gain Elevated Privileges	SECURITY
Novell Identity Manager Fan-Out Linux and UNIX Receiver Script Code Injection Vulnerability	BID
support.novell.com/cgi-bin/search/searchtid.cgi	CC
CVE Program record	CV
NVD vulnerability detail	NV

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](#)