



CVE-2017-9285

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

Summary

CVE	CVE-2017-9285
State	PUBLIC
Assigner	security@suse.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2018-03-02 20:29:00 UTC
Updated	2023-11-07 02:50:00 UTC
Description	NetIQ eDirectory before 9.0 SP4 did not enforce login restrictions when "ebaclient" was used, allowing unpermitted access

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Microfocus	Edirectory	All	All	All	All
Application	Netiq	Edirectory	9.0	sp1	All	All
Application	Netiq	Edirectory	9.0	sp2	All	All
Application	Netiq	Edirectory	9.0	sp3	All	All
Application	Netiq	Edirectory	9.0	sp1	All	All
Application	Netiq	Edirectory	9.0	sp2	All	All
Application	Netiq	Edirectory	9.0	sp3	All	All
Application	Netiq	Edirectory	All	All	All	All

References

Reference	Source	Link	Tags
Access Denied		bugzilla.suse.com	
www.novell.com/support/kb/doc.php	CONFIRM	www.novell.com	Third Party Advisory
NetIQ eDirectory 9.0 SP4 Release Notes	CONFIRM	www.netiq.com	Vendor Advisory
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)