



CVE-2015-7294

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

Summary

CVE	CVE-2015-7294
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-09-06 21:29:00 UTC
Updated	2020-03-09 18:39:00 UTC
Description	ldapauth-fork before 2.3.3 allows remote attackers to perform LDAP injection attacks via a crafted username.

Risk And Classification

Problem Types: CWE-90

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Ldapauth-fork Project	Ldapauth-fork	All	All	All	All
Application	Ldapauth-fork Project	Ldapauth-fork	All	All	All	All

References

Reference	Source	Link	Tags
oss-security - Re: CVE request - ldapauth-fork versions < 2.3.3 are vulnerable to ldap injection.	MLIST	www.openwall.com	Mailing L
oss-security - Re: CVE request - ldapauth-fork versions < 2.3.3 are vulnerable to ldap injection.	MLIST	www.openwall.com	Mailing L
Sanitize user input · vesse/node-ldapauth-fork@3feea43 · GitHub	CONFIRM	github.com	Patch, Th
Vulnerable to ldap injection · Issue #21 · vesse/node-ldapauth-fork · GitHub	CONFIRM	github.com	Third Par
CVE Program record	CVE.ORG	www.cve.org	canonica
NVD vulnerability detail	NVD	nvd.nist.gov	canonica

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

980718 Nodejs (npm) Security Update for ldapauth (GHSA-82mg-x548-gq3j)

© [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](#)