



CVE-2023-28862

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF !\[\]\(003082e50e3009141f59bd5df831749f_img.jpg\)](#)

Summary

CVE	CVE-2023-28862
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-31 17:15:00 UTC
Updated	2023-07-14 13:15:00 UTC
Description	An issue was discovered in LemonLDAP::NG before 2.16.1. Weak session ID generation in the AuthBasic handler and inco

Risk And Classification

Problem Types: CWE-287

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Lemonldap-ng	Lemonldap	\	ng	All	All

References

Reference	Source
[SECURITY] [DLA 3496-1] lemonldap-ng security update	MLIST
Version 2.16.1 · LemonLDAP NG / lemonldap-ng · GitLab	CONFID
[Security][CVE-2023-28862] AuthBasic does not handle failure correctly (#2896) · Issues · LemonLDAP NG / lemonldap-ng · GitLab	MISC
CVE Program record	CVE.ORG
NVD vulnerability detail	NVD

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

181850 Debian Security Update for lemonldap-ng (CVE-2023-28862)

6000114 Debian Security Update for lemonldap-ng (DLA 3496-1)

© [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](#)