



CVE-2021-35472

Published on: 07/27/2021 12:00:00 AM UTC

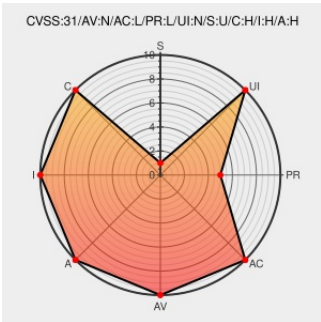
Last Modified on: 08/11/2021 03:31:00 PM UTC

CVE-2021-35472

Source: Mitre

Source: Nist

Print: PDF



Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

An issue was discovered in LemonLDAP::NG before 2.0.12. Session cache corruption can lead to authorization bypass or spoofing. By running a loop that makes many authentication attempts, an attacker might alternately be authenticated as one of two different users.

CVE-2021-35472 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **8.8 - HIGH**

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	NONE
Scope	Confidentiality Impact	Integrity Impact	Availability Impact
UNCHANGED	HIGH	HIGH	HIGH

CVSS2 Score: **6 - MEDIUM**

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE
Confidentiality Impact	Integrity Impact	Availability Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
Tags · LemonLDAP NG / lemonldap-ng · GitLab	gitlab.ow2.org text/html	MISC gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/tags
Upgrade notes for 2.0.12 (8d3b763b) · Commits · LemonLDAP NG / lemonldap-ng · GitLab	gitlab.ow2.org text/html	CONFIRM gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-

[security:high, CVE-2021-35472] session cache corruption can lead to authorization bypass or spoofing (#2539) · Issues · LemonLDAP NG / lemonldap-ng · GitLab

gitlab.ow2.org
text/html

MISC gitlab.ow2.org/lemonldap-ng/lemonldap-ng/-/issues/2539

Debian -- Security Information -- DSA-4943-1 lemonldap-ng

www.debian.org
Deprecated Link
text/html

DEBIAN DSA-4943

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

178720 Debian Security Update for lemonldap-ng (DSA 4943-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	10.0	All	All	All
Application	Lemonldap-ng	Lemonldap	\	ng	All	All
cpe:2.3:o:debian:debian_linux:10.0:*:*:*:*:*:						
cpe:2.3:a:lemonldap-ng:lemonldap:\:\:ng:*:*:*:*:						

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-35472 : An issue was discovered in LemonLDAP::NG before 2.0.12. Session cache corruption can lead to autho... twitter.com/i/web/status/1...	2021-07-27 07:46:54
@LinInfoSec	Lemonldap - CVE-2021-35472: gitlab.ow2.org/lemonldap-ng/l...	2021-07-30 16:35:11

← Previous ID

Next ID →

© CVE.report 2021 |

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](https://www.mitre.org/) and the authoritative source of CVE content is [MITRE's CVE web site](https://www.mitre.org/cve/). This site includes MITRE data granted under the following [license](https://www.mitre.org/licenses/).

CVE.report and Source URL Uptime Status status.cve.report