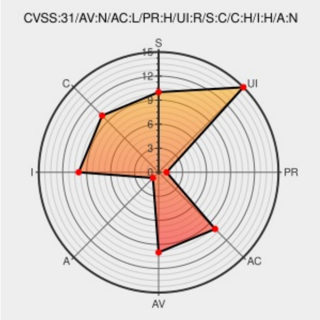
CVE-2022-24851

Published on: Not Yet Published

Last Modified on: 10/07/2022 03:21:00 PM UTC

CVE-2022-24851 - advisory for GHSA-f2fr-cccr-583v

Source: Mitre Source: NIST CVE.ORG Print: PDF



Certain versions of Debian Linux from Debian contain the following vulnerability:

LDAP Account Manager (LAM) is an open source web frontend for managing entries stored in an LDAP directory. The profile editor tool has an edit profile functionality, the parameters on this page are not properly sanitized and hence leads to stored XSS attacks. An authenticated user can store XSS payloads in the profiles, which gets triggered when any other user try to access the edit profile page. The pdf editor tool has an edit pdf profile functionality, the logoFile parameter in it is not properly sanitized and an user can enter relative paths like ../../../../../../../../../../../../../usr/share/icons/hicolor/48x48/apps/gvim.png via tools like burpsuite. Later when a pdf is exported using the edited profile the pdf icon has the image on that path(if image is present). Both issues require an attacker to be able to login to LAM admin interface. The issue is fixed in version 7.9.1.

CVE-2022-24851 has been assigned by security-advisories@github.com to track the vulnerability - currently rated as MEDIUM severity.

Affected Vendor/Software: **LDAPAccountManager** - **lam** version < **7.9.1**

CVSS3 Score: 4.8 - MEDIUM

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

CVSS2 Score: 3.5 - LOW

Access Vector	Access Complexity	Authentication
NETWORK	MEDIUM	SINGLE

Confidentiality Impact	Integrity Impact	Availability Impact
NONE	PARTIAL	NONE

CVE References

Description	Tags	Link
Stored XSS and arbitrary image read vulnerability · Advisory · LDAPAccountManager/lam · GitHub	github.com text/html	CONFIRM github.com/LDAPAccountManager/lam/security/advisories/GHSA-f2
Multiple vulnerabilities in LDAP Account Manager · Issue #170 · LDAPAccountManager/lam · GitHub	github.com text/html	MISC github.com/LDAPAccountManager/lam/issues/170
Debian -- Security Information -- DSA-5177-1 ldap-account-manager	www.debian.org Depreciated Link text/html	DEBIAN DSA-5177
#170 fixed security issues in profile editor and PDF editor · LDAPAccountManager/lam@3c6f09a · GitHub	github.com text/html	MISC github.com/LDAPAccountManager/lam/commit/3c6f09a3579e048e224eb5a4c4e3e

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

180808 Debian Security Update for ldap-account-manager (DSA 5177-1)

730468 LDAP Account Manager Stored Cross-Site Scripting (XSS) and Arbitrary Image Read Vulnerability

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	11.0	All	All	All
Application	Ldap-account-manager	Ldap Account Manager	All	All	All	All

cpe:2.3:o:debian:debian_linux:11.0:*:*:*:*:*:*:*:

cpe:2.3:a:ldap-account-manager:ldap_account_manager:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2022-24851 : LDAP Account Manager LAM is an open source web frontend for managing entries stored in an LDAP d… twitter.com/i/web/status/1…	2022-04-15 18:49:57
/r/netcve	CVE-2022-24851	2022-04-15 19:39:03

← Previous ID Next ID→

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 registred 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