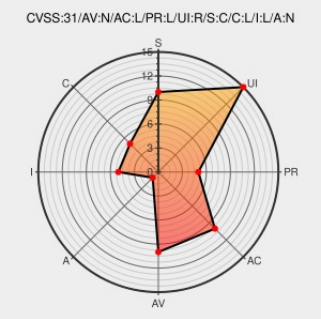
CVE-2020-7934

Published on: 01/28/2020 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:23:54 PM UTC

CVE-2020-7934

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



Certain versions of Liferay Portal from Liferay contain the following vulnerability:

In LifeRay Portal CE 7.1.0 through 7.2.1 GA2, the First Name, Middle Name, and Last Name fields for user accounts in MyAccountPortlet are all vulnerable to a persistent XSS issue. Any user can modify these fields with a particular XSS payload, and it will be stored in the database. The payload will then be rendered when a user utilizes the search feature to search for other users (i.e., if a user with modified fields occurs in the search results). This issue was fixed in Liferay Portal CE version 7.3.0 GA1.

CVE-2020-7934 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.4 - MEDIUM

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	LOW	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
GitHub - 2ndC4me/liferay-xss-7.2.1GA2-poc-report-CVE-2020		MISC github.com/2ndC4me/liferay-xss

GitHub - 3ndG4me/liferay-xss-7.2.1GA2-poc-report-CVE-2020-7934: Authenticated Stored XSS in LifeRay 7.2.0 GA1 via MyAccountPortlet executed by Search Results	github.com text/html	MISC github.com/3ndG4me/liferay-xss-7.2.1GA2-poc-report-CVE-2020-7934
LifeRay 7.2.1 GA2 Cross Site Scripting ≈ Packet Storm	packetstormsecurity.com text/html	MISC packetstormsecurity.com/files/160168/LifeRay-7.2.1-GA2-Cross-Site-Scripting.html
Liferay Portal Authenticated XSS Public Vulnerability Disclosure (CVE-2020-7934) – SemanticBits	Third Party Advisory semanticbits.com text/html	MISC semanticbits.com/liferay-portal-authenticated-xss-disclosure/

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.

There are currently no QIDs associated with this CVE

Exploit/POC from Github

Authenticated Stored XSS in LifeRay 7.2.0 GA1 via MyAccountPortlet executed by Search Results

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Liferay	Liferay Portal	All	All	All	All

cpe:2.3:a:liferay:liferay_portal:*:*:*:*:community:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→