CERT-EU

Security Advisory 2023-082

Multiple Vulnerabilities in LifeRay products

October 26, 2023 — v1.0

TLP:CLEAR

History:

- *26/10/2023 — v1.0 – Initial publication*

Summary

This security advisory addresses multiple vulnerabilities in Liferay Portal and Liferay DXP related to cross-site scripting (XSS) attacks [1]. Users are urged to update their installations to the latest versions as provided in the "Recommendations" section.

Technical Details

The vulnerabilities are described as follows:

1. **CVE-2023-44311 - Reflected XSS with 'code' and 'error' in OAuth2ProviderApplicationRedirect**: This vulnerability, with a CVSS score of 9.6, allows remote attackers to inject arbitrary web script or HTML via the `code`, or `error` parameter [2].
2. **CVE-2023-42628 - XSS with child wiki pages**: This vulnerability, with a CVSS score of 9.0, allows remote attackers to inject arbitrary web script or HTML into a parent wiki page via a crafted payload injected into a wiki page's 'Content' text field [3].
3. **CVE-2023-42627 - Multiple stored XSS with shipping & billing address**: This vulnerability, with a CVSS score of 9.6, allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into multiple fields in the Commerce module [4].
4. **CVE-2023-42497 - XSS with `redirect` in export translation**: This vulnerability, with a CVSS score of 9.6, allows remote attackers to inject arbitrary web script or HTML via the `_com_liferay_translation_web_internal_portlet_TranslationPortlet_redirect` parameter [5].
5. **CVE-2023-42629 - Stored XSS vulnerability with vocabulary description**: This vulnerability, with a CVSS score of 9.0, allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into a Vocabulary's `description` text field [6].
6. **CVE-2023-44310 - XSS with page name in Page Tree**: This vulnerability, with a CVSS score of 9.0, allows remote attackers to inject arbitrary web script or HTML via a crafted payload injected into page's `Name` text field.

Affected Products

These vulnerabilities affect Liferay DXP and Liferay Portal. Please refer to the individual CVE details above.

Recommendations

Users running affected versions should update to the latest versions available.

References

[1] https://liferay.dev/portal/security/known-vulnerabilities

[2] https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44311

[3] https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42628

[4] https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42627

[5] https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42497

[6] https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-42629

[7] https://liferay.dev/portal/security/known-vulnerabilities/-/asset_publisher/jekt/content/cve-2023-44310