Liferay Security Development Overview

How Liferay Approaches Security

Liferay®

Executive Summary

Liferay is committed to producing secure, high quality products for our customers. Best practices for security are incorporated into our development process (rather than being addressed after the fact), and we continually test our software against industry standards to ensure it meets a broad range of requirements. In addition, our security team works to identify vulnerabilities and provides rapid notification of issues, bug resolution and transmission of the bug fix to Liferay customers. Our goal is to take care of security concerns as quickly as possible, so our customers can focus their efforts on running their business.

Liferay products and technologies are a trusted choice for many security-conscious government entities and industries, including various military organizations, financial services and healthcare. Liferay Digital Experience Platform (DXP) is ISO/IEC 27001:2013 certified and enables customers to develop websites that are flexible enough to meet changing compliance standards.

This document provides an overview of the processes used during development and testing of Liferay products. Combined, these processes ensure that Liferay's customers can have confidence in the security and ongoing reliability of Liferay products, including Liferay Digital Experience Platform, Liferay Experience Cloud, and Liferay Experience Cloud Self-Managed.

Liferay Secure Development Process

To ensure that our software has minimal vulnerabilities, Liferay uses a holistic security approach. Our engineering team:

1. Performs background checks on all new members.
2. Receives training on general security awareness, secure coding best practices, and how to design software with security in mind.
3. Receives training multiple times a year to recognize and report phishing attacks.
4. Uses state-of-the-art XDR antimalware solution, password manager, MFA and password-protected SSH keys to access and commit to code repositories.
5. Enforces multiple layers of code reviews with only a limited number of privileged accounts having access to commit code to the main repository.
6. Develops according to secure coding best practices and guidelines such as OWASP Cheat Sheet project, the OWASP Top 10, and the CWE/SANS Top 25.

7. Relies on an internal DXP security framework consisting of various security utilities for passwords, encryption, sanitization, input validation, and output escaping as well as larger frameworks for permission checking, various pluggable authentication layers for session and/or API based access and other secured and reviewed code infrastructure in order to avoid vulnerabilities.
8. Dedicates an application security team to implement, review, and maintain security related code.
9. Utilizes internal code security audits, SCA scanning, antivirus testing, internal and external penetration testing, as well as static and dynamic scans to hunt for vulnerabilities.
10. Follows a notification, triage, and resolution strategy to resolve security vulnerabilities in a timely manner.

OWASP and CWE/SANS

Liferay follows the OWASP Top 10 (2017) and CWE/SANS Top 25 lists to ensure that Liferay DXP meets the security requirements necessary for protecting enterprises against known vulnerabilities and attacks. For example:

- Liferay DXP's persistence layer is generated and maintained by parameter-based queries and the Service Builder framework, which prevents HQL and SQL Injection using Hibernate.
- To prevent Cross Site Scripting (XSS), user-submitted values are contextually escaped on output.
- User input is validated using business logic constraints and checked for type safety to prevent deserialization attacks. Where required, content is sanitized and dangerous characters are removed.
- To support integration features, Liferay DXP only syntactically encodes input when switching language contexts (HTML, URL encoding, LDAP encoding, SQL encoding, XML, JSON, etc). But the content is not double-encoded or otherwise changed when storing to preserve the semantics of the input.
- Liferay DXP includes built-in protection against CSRF attacks, Local File Inclusion, Open Redirects, Uploading and Serving files of dangerous types, Content Sniffing, Clickjacking, Path Traversal, and many other common attacks.

To protect against less common vulnerabilities, Liferay DXP also contains fixes for state-of-the-art attacks and techniques to improve product security. For example, Liferay DXP uses PBKDF2 to store passwords. Liferay DXP also contains mitigation for various OAuth2 attacks, XXE attack, Reflected File Download, and other kinds of attacks.

Security Testing and Verification

Our process for continuous testing includes:

1. Security tests in the form of code unit tests, integration tests and automated in-browser testing of security features.
2. Security code reviews.
3. Continuous scan of open-source dependencies, white and black box security scans from a market leading third-party application security firms.
4. Penetration testing by independent third parties on every major release.
5. Security program for reporting security vulnerabilities by the open source community, customers and independent security researchers.
6. Continuous vulnerability monitoring of third-party libraries included in Liferay products.

Liferay does not simply use a third-party service for dynamic and static analysis. Liferay uses a process defined by a third party for rating and ranking the security of its products. This provides an additional set of independent controls to ensure a proper level of vulnerability testing for Liferay products.

Liferay DXP Release Process

The product release process:

1. Is isolated in a separate monitored environment with access granted only to a few selected engineers.
2. Is automated to prevent manual errors.
3. Undergoes manual and automated testing.
4. Includes release notes where every fixed vulnerability is assigned a unique identifier.
5. Security vulnerabilities are assigned a Mitre's CVE number.
6. Customer notification for important security releases and security updates.

Liferay DXP docker image releases are tested on top for image vulnerabilities.

External Security Analysis of Liferay

Liferay DXP leverages open source code that has gone through comprehensive testing cycles, intensive external analysis, and performance tuning in order to make it ready for business-critical use cases.

With focus purely on external security audits of the software, Liferay DXP is continuously scanned and tested throughout the year for vulnerabilities using Checkmarx CxSAST and Rapid7 InsightAppSec, leading providers of application risk assessments. The DAST tests perform over 2 million attacks on the application in each run. SAST testing categories include tests for OWASP ASVS, OWASP Top 10 2021 + 2017 + 2013 + 2010, OWASP Top 10 API, CWE top 25, SANS top 25, FISMA 2014, NIST SP 800-53, PCI DSS v3.2.1, OWASP Mobile Top 10 2016 and others. All these tests were expanded in 2022 to cover DXP supported versions down to Liferay Portal Enterprise Edition 6.2, including Liferay docker releases, where available. In addition, Liferay DXP is tested by an external penetration testing company on a yearly basis, customers and community researchers as part of a responsible disclosure program.

Additionally, Liferay is a ISO/IEC 27001:2013 certified provider whose Information Security Management System (ISMS) has received third-party accreditation from the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC).

Our cloud offerings, Liferay Experience Cloud and Liferay Experience Cloud Self-Managed, have 250 internal controls and numerous certifications from third-party vendors.

Our infrastructure compliance program includes:

- SOC 2 Type 1 & 2 Certification
- ISO/IEC 27001:2013 Certification
- ISO/IEC 27017:2015 Certification
- ISO/IEC 27018:2019 Certification
- HIPAA
- CSA Star Level 2

These independent third-party security reports mean that Liferay has undergone rigorous testing based on the most widely accepted and comprehensive methods to ensure that the platform meets customer requirements for addressing security issues in an effective and proactive manner.

Security Incident Response

When potential security vulnerabilities are found by Liferay's security team, security testing vendors or customers, we:

1. Classify the severity of the vulnerability.
2. Triage and resolve the vulnerability.
3. Assign CVE number and CVSSv3 scoring.
4. Notify our Enterprise Subscription customers and provide them with a security update/fix pack.
5. If appropriate, notify our open source community users and provide them with a security update.

More details of this process can be found at liferay.com/security.

Conclusion

As threats to cybersecurity continue to rise, maintaining software security will require continuous evaluation and testing from security experts. Software security is not a matter of building a wall strong enough to hold against every attack. It requires something closer to an immune system, a process for reviewing and addressing new issues as efficiently as possible. Through our dedicated, systematic approach to security in the development and testing process, Liferay ensures our products adhere to the most up-to-date security standards and continues to provide highly secure products to our customers.

Moving Forward

Schedule a Free Demo

A Liferay team member is available to give you an in-depth look at the features and solutions possible with the latest version of Liferay DXP. Our customers include top global companies across industries such as Airbus, Hewlett Packard Enterprise, and Volkswagen.

Request a free demo by visiting liferay.com/request-a-demo.

Liferay makes software that helps companies create digital experiences on web, mobile and connected devices. Our platform is open source, which makes it more reliable, innovative and secure. We try to leave a positive mark on the world through business and technology. Hundreds of organizations in financial services, healthcare, government, insurance, retail, manufacturing and multiple other industries use Liferay. Visit us at liferay.com.

221216