



472

VULNERABILITIES SUBMITTED SINCE LAUNCH

98

VULNERABILITIES FOR THE MONTH

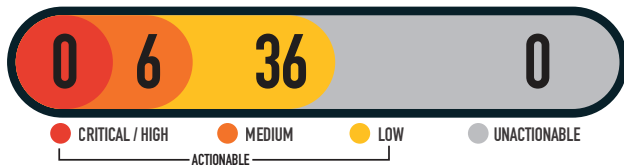
118

RESEARCHERS SINCE LAUNCH

42

ACTIONABLE REPORTS PROCESSED

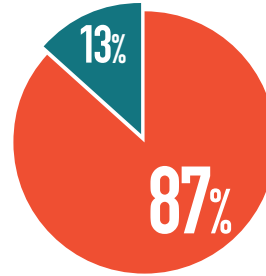
## SEVERITY FOR THE MONTH



● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE



MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH



## MITIGATIONS FOR THE MONTH


- 26 Successful Mitigations (Including Top 5 Organization Data)
- 4 Unsuccessful Attempts

## KNOWLEDGE BYTE

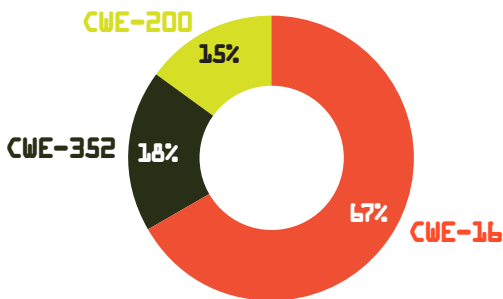
In September 2024, the DoD VDP received a critical severity submission demonstrating the potential for Remote Code Execution within unpatched versions of the Liferay software. Liferay Portal is an enterprise package used for content management and development. Researchers displayed the possibility of executing custom commands within the software by injecting specific serialized data payloads. System owners deploying Liferay software are encouraged to review and update any affected versions. Further information is available in the following resources:

- <https://nvd.nist.gov/vuln/detail/CVE-2020-7961>
- <https://codewhitesec.blogspot.com/2020/03/liferay-portal-json-vulns.html>
- [https://cheatsheetseries.owasp.org/cheatsheets/Deserialization\\_Cheat\\_Sheet.html](https://cheatsheetseries.owasp.org/cheatsheets/Deserialization_Cheat_Sheet.html)

## RESEARCHER OF THE MONTH

 **Vulnerability Alert!** Liferay Portal (pre-7.2.1 CE GA2) is vulnerable to remote code execution through deserialization of untrusted data in JSON web services (JSONWS). Huge thanks to @exploit\_msf for the discovery! Patch immediately. #CyberSecurity #InfoSec #LiferayPortal

## VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE- 116 MISCONFIGURATION: 18  
 CWE-352 CROSS-SITE REQUEST FORGERY (CSRF): 5  
 CWE-200 INFORMATION DISCLOSURE: 4

## TOP VULNERABILITIES SINCE LAUNCH

- 59 CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES
- 24 CWE- 79 CROSS-SITE SCRIPTING (XSS)
- 22 CWE-200 INFORMATION DISCLOSURE

