DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES SEPTEMBER 2024

DOD CYBER CRIME CENTER

53,084
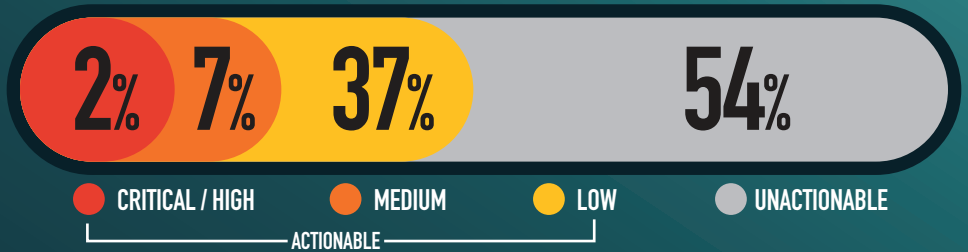VULNERABILITIES SINCE LAUNCH

6,764
RESEARCHERS SINCE LAUNCH
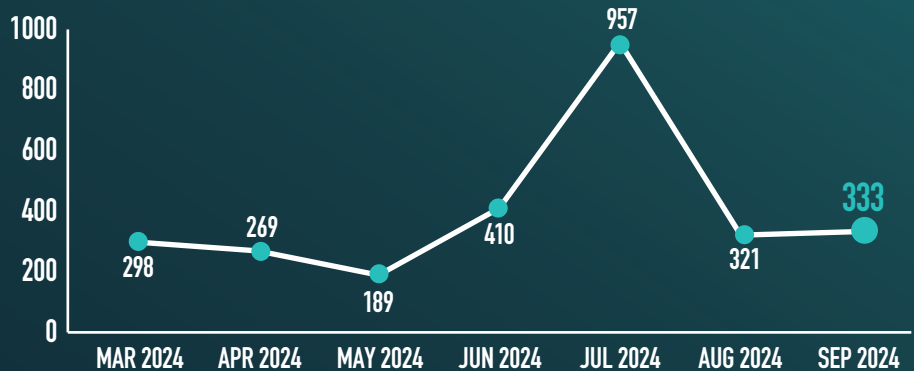
29,293
ACTIONABLE REPORTS PROCESSED

161
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH

2%	7%	37%	54%

● CRITICAL / HIGH   ● MEDIUM   ● LOW   ● UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

	MAR 2024	APR 2024	MAY 2024	JUN 2024	JUL 2024	AUG 2024	SEP 2024
Value	298	269	189	410	957	321	333

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE — 71

CWE-284 IMPROPER ACCESS CONTROL - GENERIC — 30

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 25

CWE-79 CROSS-SITE SCRIPTING — 19

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

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

DC3 DOD CYBER CRIME CENTER