



51,272

VULNERABILITIES SINCE LAUNCH

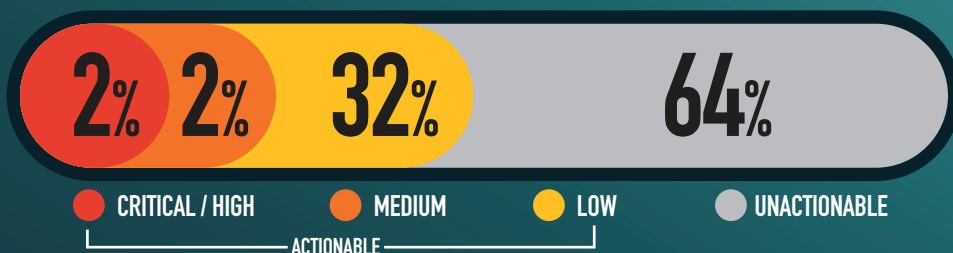
6,286

RESEARCHERS SINCE LAUNCH

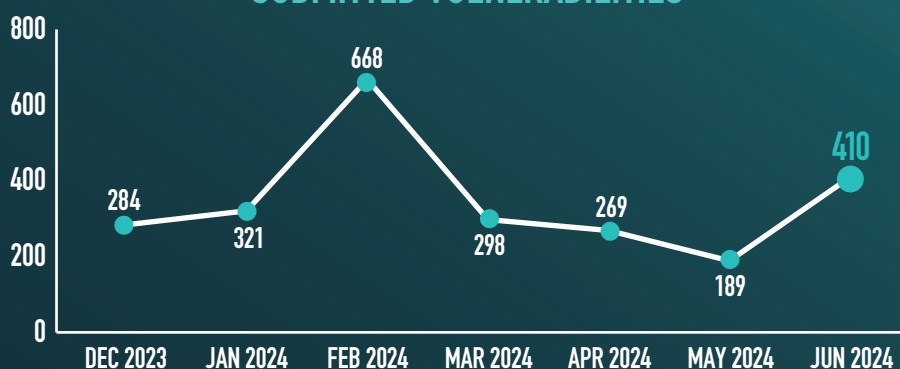
28,654

ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES 95

CWE-200 INFORMATION DISCLOSURE 43

CWE-644 IMPROPER NEUTRALIZATION OF HTTP HEADERS FOR SCRIPTING SYNTAX 16

CWE-601 OPEN REDIRECT 14

KNOWLEDGE BYTE

In June 2024, the DoD VDP received multiple high-severity submissions outlining XML External Entity (XXE) injection. XML is a format used for transmitting data that allows for self-defined structures. By exploiting these self-defined structures, it is possible to have a server processing the requests return information outside of the intended scope. Researchers were able to craft a custom request which, when processed by the server, could potentially expose critical operating system files. System owners are encouraged to evaluate their XML parsers and disable any features not required. Further information is available in the following resources: <https://portswigger.net/web-security/xxe> & https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html & <https://research.nccgroup.com/wp-content/uploads/2020/09/VSRL-XMLDTDEntityAttacks.pdf>

RESEARCHER OF THE MONTH

🔒 Cybersecurity Alert! 🗣️ @Orange_303_ has identified a critical vulnerability in Oracle WebLogic Server (CVSS 9.8). This flaw allows unauthenticated attackers to take over servers via HTTP. Ensure your systems are patched to protect your data! #CyberSecurity #InfoSec #OracleWebLogic