



516

VULNERABILITIES
SUBMITTED
SINCE LAUNCH

44

VULNERABILITIES
FOR THE MONTH

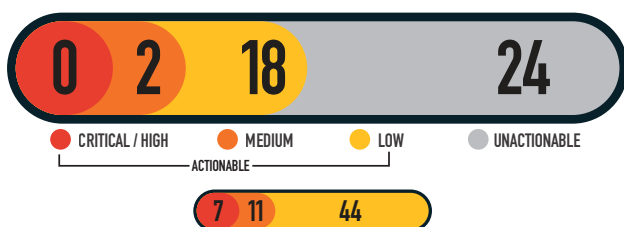
131

RESEARCHERS
SINCE LAUNCH

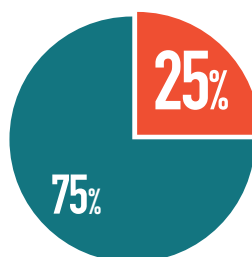
20

ACTIONABLE
REPORTS
PROCESSED

SEVERITY FOR THE MONTH



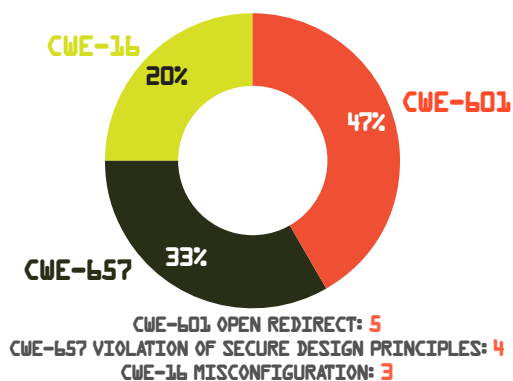
MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH



MITIGATIONS FOR THE MONTH

- 1 Successful Mitigations (Including Top 5 Organization Data)
- 3 Unsuccessful Attempts

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



KNOWLEDGE BYTE

In October 2024, the DIB-VDP received a submission demonstrating the potential for a Blind Server-Side Request Forger (SSRF) and Denial of Service (DOS) within a xmlrpc.php WordPress file. The eXtensible Markup Language Remote Procedure Call (XMLRPC) is a protocol that allows software to communicate with each other over the internet using remote procedure calls. Within the report the researchers displayed the possibility of executing commands within the page by bypassing input validation, sending a POST request to the server. System owners are encouraged to disable xmlrpc or turn off pingback, this is dependent on system needs. Further information is available: <https://nvd.nist.gov/vuln/detail/CVE-2022-47514>

https://cheatsheetseries.owasp.org/cheatsheets/XML_External_Entity_Prevention_Cheat_Sheet.html

RESEARCHER OF THE MONTH

Security Alert! by @leoanggal1: XSS vulnerability discovered allowing unauthorized injection through arbitrary JavaScript actions to be executed via crafted script. This critical flaw could enable attackers to gather sensitive data without authentication. Immediate patching and sanitization of allowable characters are advised! #DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH

