DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES DECEMBER 2025

58,451
VULNERABILITIES SINCE LAUNCH

7,911
RESEARCHERS SINCE LAUNCH

31,614
ACTIONABLE REPORTS PROCESSED

166
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH

2% **14%** **23%** **61%**

- CRITICAL / HIGH
- MEDIUM
- LOW
- UNACTIONABLE

ACTIONABLE
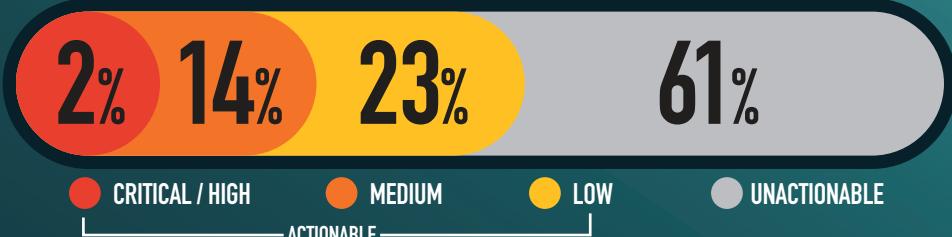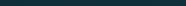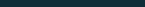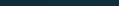
SUBMITTED VULNERABILITIES

388	414	300	349	409	232	398
JUN 2025	JUL 2025	AUG 2025	SEP 2025	OCT 2025	NOV 2025	DEC 2025

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

- CWE-200 INFORMATION DISCLOSURE — 193
- CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 33
- CWE-284 IMPROPER ACCESS CONTROL - GENERIC — 13
- CWE-79 CROSS-SITE SCRIPTING — 10
- CWE-601 OPEN REDIRECT — 9

KNOWLEDGE BYTE

In December 2025, the DoD VDP received multiple critical severity submissions identifying CVE-2025-55182, an unauthenticated remote code execution vulnerability within React Server Components. React is a popular JavaScript library used for developing web applications. Researchers identified a flaw in parts of the library that allowed custom-crafted HTTP requests to be deserialized and processed directly by the web server. It is recommended that all system owners update to the latest approved React library. Further information is available in the following resources:

https://nvd.nist.gov/vuln/detail/CVE-2025-55182
https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components
https://unit42.paloaltonetworks.com/cve-2025-55182-react-and-cve-2025-66478-next/

RESEARCHER OF THE MONTH

Huge congratulations to **@wgujjer11** for being named Researcher of the Month. **@wgujjer11** is being recognized for finding a Remote Code Execution vulnerability related to React Server (React2Shell), which could have led to remote execution of system commands on the target server. Well deserved**! #CyberSecurity #VDP**