DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE DECEMBER 2025

DIB-VDP

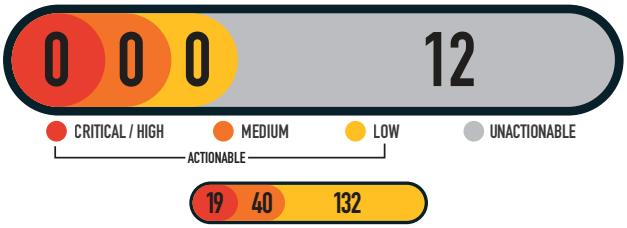
977
VULNERABILITIES SUBMITTED
SINCE LAUNCH

10
VULNERABILITIES
FOR THE MONTH

258
RESEARCHERS
SINCE LAUNCH

0
ACTIONABLE REPORTS
PROCESSED

SEVERITY FOR THE MONTH

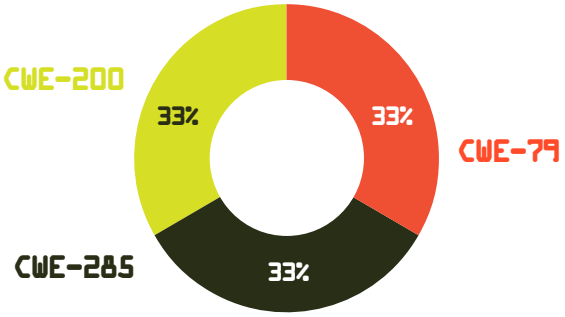


MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH

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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-79 CROSS-SITE SCRIPTING XSS: 0
CWE-285 IMPROPER AUTHORIZATION: 0
CWE-200 INFORMATION DISCLOSURE: 0

KNOWLEDGE BYTE

In December 2025, the DIB-VDP observed industry reporting on React2Shell, a critical remote code execution vulnerability impacting applications using React Server Components. The vulnerability stems from improper validation and handling of server-side component requests, allowing unauthenticated attackers to inject and execute arbitrary code within the application runtime. Successful exploitation could lead to full server compromise, data exfiltration, and abuse of downstream services and supply-chain dependencies. Further technical details and guidance are available in the following resources:

https://github.com/advisories
https://securityboulevard.com
https://www.cisa.gov/known-exploited-vulnerabilities

TOP VULNERABILITIES SINCE LAUNCH