DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE FEBRUARY 2026

DIB-VDP

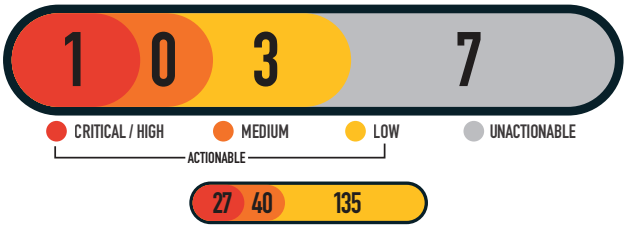
1011 VULNERABILITIES SUBMITTED SINCE LAUNCH

11 VULNERABILITIES FOR THE MONTH

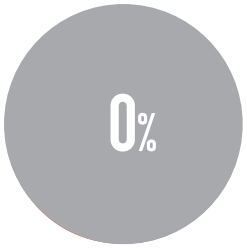
284 RESEARCHERS SINCE LAUNCH

4 ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



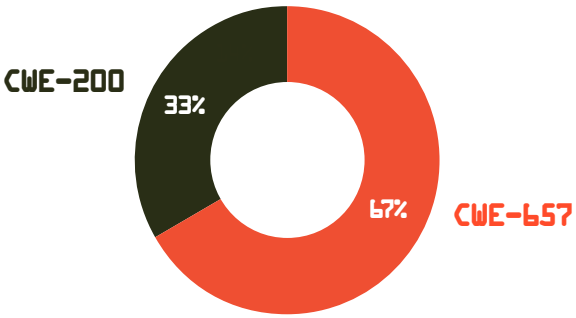
MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH



MITIGATIONS FOR THE MONTH

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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 2
CWE-200 INFORMATION DISCLOSURE: 1

KNOWLEDGE BYTE

In February 2026, the DIB-VDP received a critical issue highlighted this month demonstrates the severe risk posed by Server-Side Template Injection (SSTI). When user input is embedded directly into server-side template engines without proper sanitization, attackers can manipulate template logic and potentially achieve remote code execution. Successful exploitation can expose sensitive data, environment variables, and credentials – and in worst cases, lead to full server compromise. Strict input validation, proper context-aware escaping, and secure template configuration are essential to prevent this high-impact vulnerability. Further information is available in the following resources:

https://owasp.org/www-community/attacks/Server-Side_Template_Injection
https://portswigger.net/web-security/server-side-template-injection
https://cwe.mitre.org/data/definitions/94.html

RESEARCHER OF THE MONTH

Shoutout to @kaanmert9 for uncovering an SSTI vulnerability on /contact-us/ where user input could trigger arbitrary code execution. Exploits like this can lead to server takeover, data theft, and lateral movement. Great catch protecting the ecosystem! #DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH