DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE

SEPTEMBER 2025

DIB-VDP

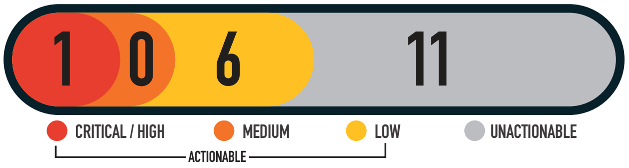
912 VULNERABILITIES SUBMITTED SINCE LAUNCH

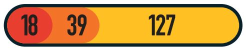
18 VULNERABILITIES FOR THE MONTH

242 RESEARCHERS SINCE LAUNCH

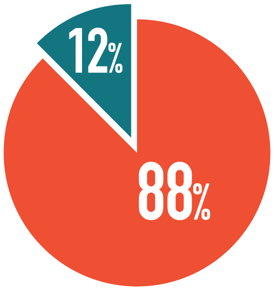
7 ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH





MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

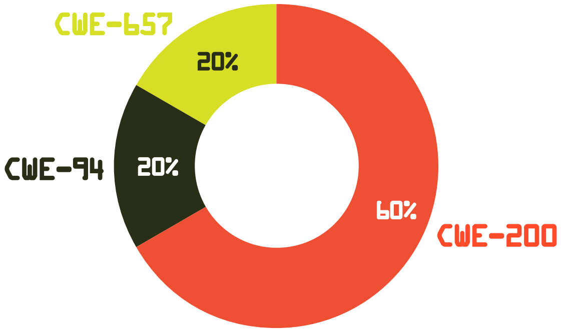


MITIGATIONS FOR THE MONTH

● 14 Successful Mitigations (Including Top 5 Organization Data)

● 2 Unsuccessful Attempts

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-200 INFORMATION DISCLOSURE: 4

CWE-94 CODE INJECTION: 1

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 1

KNOWLEDGE BYTE

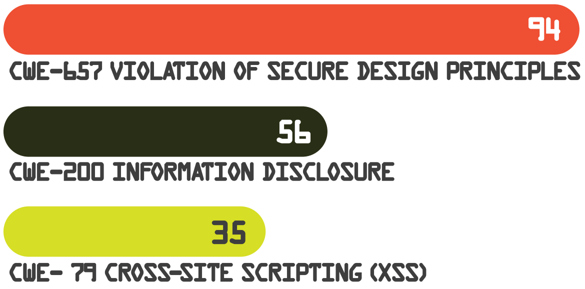
In September 2025, the DIB-VDP reported a critical Server-Side Template Injection (SSTI) vulnerability. Attackers could exploit POST requests by injecting malicious template payloads that the server-side engine evaluates, potentially allowing code execution, data theft, privilege escalation, and lateral movement across systems. The impact could extend beyond individual accounts, putting entire environments at risk. System owners are strongly advised to validate and sanitize all POST inputs, never evaluate user-controlled data in template engines, and patch or upgrade affected systems. Additional defenses include least-privilege configurations, WAF rules, and runtime monitoring. Further information is available in the following resources:

https://cheatsheetseries.owasp.org/cheatsheets/Injection_Prevention_Cheat_Sheet.html
https://cwe.mitre.org/data/definitions/94.html
https://owasp.org/www-project-web-security-testing-guide/v41/4-Web_Application_Security_Testing/07-Input_Validation_Testing/18-Testing_for_Server_Side_Template_Injection

RESEARCHER OF THE MONTH

Huge thanks to @kaanmert9 for identifying a **Server-Side Template Injection** vulnerability in our program 🎯 This critical finding highlights how SSTI can lead to full RCE and data exposure if left unchecked. #DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH



𝕏 @DC3VDP
AFOSI.DC3.DIB-VDP@us.af.mil

DoD CYBER CRIME CENTER AND
DEFENSE COUNTERINTELLIGENCE
& SECURITY AGENCY