DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE APRIL 2026

DIB-VDP

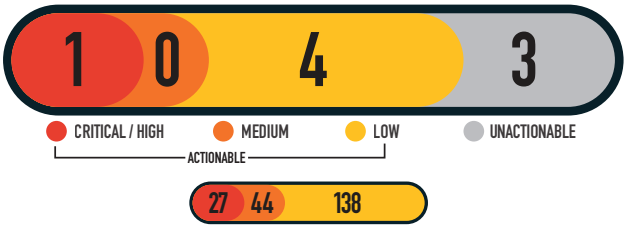
1054
VULNERABILITIES SUBMITTED SINCE LAUNCH

8
VULNERABILITIES FOR THE MONTH

289
RESEARCHERS SINCE LAUNCH

5
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

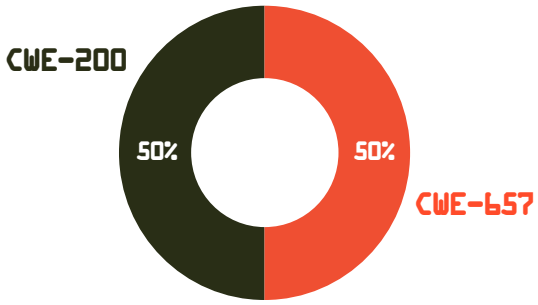


MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH

- 2 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: 1
CWE-200 INFORMATION DISCLOSURE: 1

KNOWLEDGE BYTE

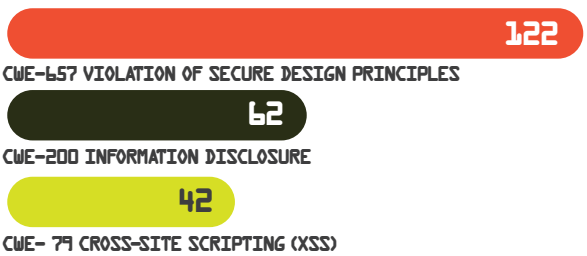
In April 2026, the DIB-VDP has observed a continued rise in vulnerability submissions related to Server-Side Template Injection (SSTI), a critical class of injection flaw affecting web applications that use template engines for dynamic content rendering. SSTI occurs when untrusted user input is embedded into server-side templates without proper sanitization, allowing attackers to manipulate template syntax. In severe cases, this can lead to remote code execution (RCE), unauthorized data access, or full system compromise within environments supporting Defense Industrial Base (DIB) operations. Due to the sensitivity of DIB systems, SSTI vulnerabilities pose a significant operational and national security risk, particularly when exposed in externally reachable applications or supply chain-integrated services. Organizations are strongly advised to validate all template rendering inputs, enforce strict context-aware output encoding, and regularly patch affected frameworks and engines. Further technical details and guidance are available in the following resources:

https://portswigger.net/web-security/server-side-template-injection
https://owasp.org/www-community/attacks/Server-Side_Template_Injection
https://nvd.nist.gov/vuln/search/results?query=server-side%20template%20injection

RESEARCHER OF THE MONTH

Big thanks to @dmDUSTBIN for the excellent discovery of an Open Redirect via Encoded Path Injection. Findings like this highlight how small URL handling flaws can lead to serious security exposure and potential phishing risk. Security research like this helps strengthen the entire DIB. **#DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking**

TOP VULNERABILITIES SINCE LAUNCH



@DC3VDP
AFOSI.DC3.DIB-VDP@us.af.mil

DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY