DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE

JULY 2025

DIB-VDP

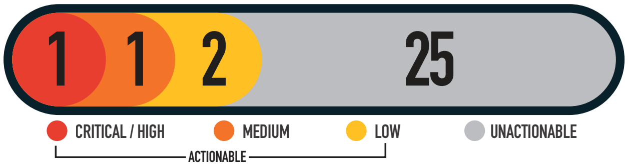
857
VULNERABILITIES SUBMITTED SINCE LAUNCH

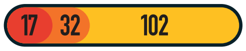
28
VULNERABILITIES FOR THE MONTH

227
RESEARCHERS SINCE LAUNCH

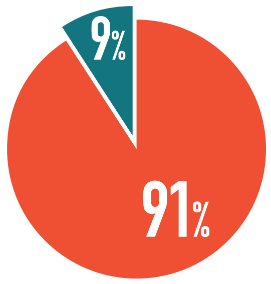
4
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH





MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

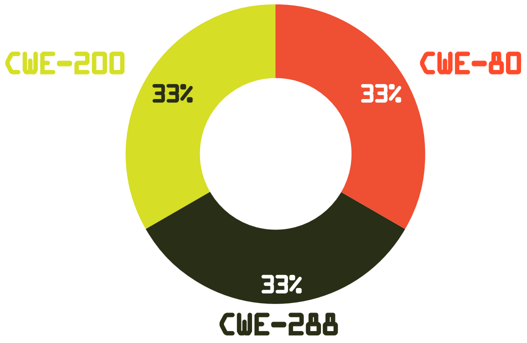


MITIGATIONS FOR THE MONTH

● 20 Successful Mitigations (Including Top 5 Organization Data)

● 2 Unsuccessful Attempts

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE- 80 IMPROPER NEUTRALIZATION OF SCRIPT-RELATED HTML TAGS IN A WEB PAGE (XSS): 1

CWE-288 AUTHENTICATION BYPASS USING A ALTERNATE PATH OR CHANNEL: 1

CWE-200 INFORMATION DISCLOSURE: 1

KNOWLEDGE BYTE

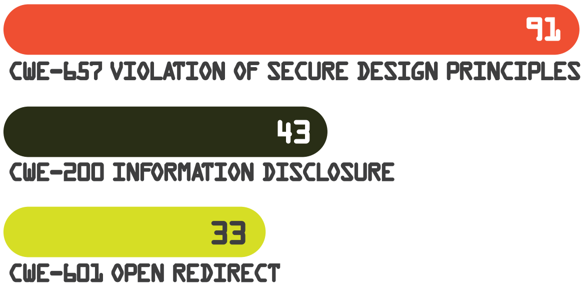
In July 2025, the DIB-VDP received a high-severity vulnerability report detailing a technique for account takeover via user credential manipulation during an authentication timing window. The vulnerability was exploited by manipulating the POST request during an extended sync delay in the login process. By intercepting and modifying specific authentication parameters mid-request, attackers could change credentials, gaining unauthorized access to accounts. System owners are encouraged to implement strict validation for all POST parameters, bind tokens tightly to validated user credentials, introduce nonce/timestamp checks to prevent replay or delay-based manipulation, and monitor for abnormal POST timing or token reuse.

Further information is available in the following resources:
https://cheatsheetseries.owasp.org/cheatsheets/Authentication_Cheat_Sheet.html
https://cwe.mitre.org/data/definitions/384.html
https://oauth.net/articles/authentication/

RESEARCHER OF THE MONTH

Shoutout to @Ha0ker for responsibly disclosing a **token generation flaw**—tokens could be created **before account sync completes**, opening the door to potential abuse. Great catch! **#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