

DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE

DECEMBER 2024

DIB-VDP



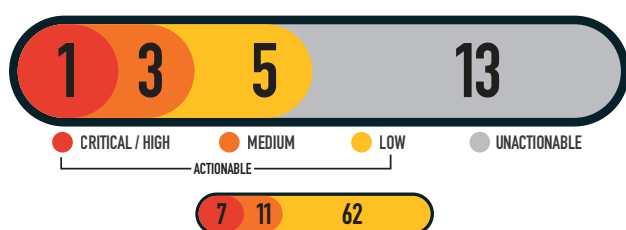
549
VULNERABILITIES
SUBMITTED
SINCE LAUNCH

22
VULNERABILITIES
FOR THE MONTH

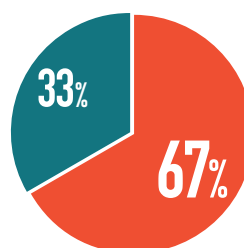
137
RESEARCHERS
SINCE LAUNCH

9
ACTIONABLE
REPORTS
PROCESSED

SEVERITY FOR THE MONTH



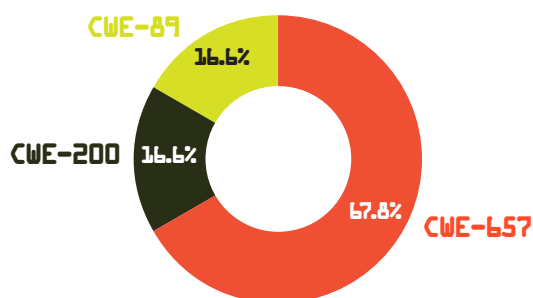
MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH



MITIGATIONS FOR THE MONTH

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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 4
CWE-200 INFORMATION DISCLOSURE: 1
CWE-89 SQL INJECTION: 1

KNOWLEDGE BYTE

In December 2024, the DIB-VDP received a submission demonstrating the potential of a SQL Injection (SQLi) vulnerability. SQLi could allow an unauthenticated adversary to view, tamper with or destroy sensitive data stored within a database. System owners are encouraged to perform one of the following: use of prepared statements, use of properly constructed stored procedures, allow-list Input validation, and/or escape all user input before ingestion.

Further information is available in the following resources:

https://owasp.org/www-community/attacks/SQL_Injection

https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html

RESEARCHER OF THE MONTH

Shoutout to [@Grammatic](#) for identifying SQL injection risks. SQLi vulnerabilities can lead to data breaches and compromised systems. It's vital to address them promptly. #DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH

