DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM
MYTE BYTE FEBRUARY 2025
DIB-VDP

696 VULNERABILITIES SUBMITTED SINCE LAUNCH
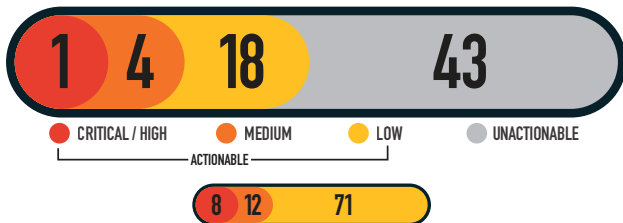
66 VULNERABILITIES FOR THE MONTH
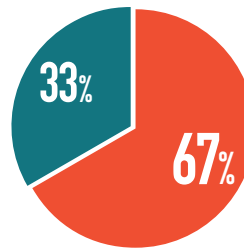
165 RESEARCHERS SINCE LAUNCH

23 ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

1 CRITICAL / HIGH   **4** MEDIUM   **18** LOW   **43** UNACTIONABLE

ACTIONABLE
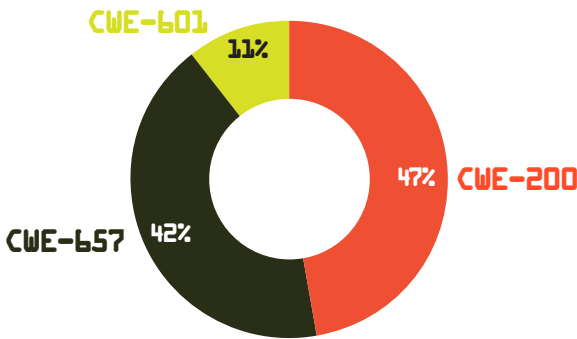
8 **12** **71**

MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH

33% 67%

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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH

CWE-601 — 11%
CWE-657 — 42%
CWE-200 — 47%

CWE-200 INFORMATION : **9**
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: **8**
CWE-601 OPEN REDIRECT: **2**

KNOWLEDGE BYTE

In February 2025, the DIB-VDP received a submission demonstrating the potential for a Personally Identifiable Information (PII) Leak through a publicly accessible Unauthorized Page. The page could allow an attacker to access sensitive data, compromising the system owner and users. This particular vulnerability can be found through reconnaissance or common mapping tools. It is critical to check all publicly accessible web pages and applications for inappropriate access control which could result in unintended disclosure of sensitive data. Further information is available in the following resources:

https://wiki.owasp.org/images/7/75/Owasp-nist-sp-800-122.pdf

https://medium.com/@ar_hawk/how-a-simple-directory-listing-leads-to-pii-data-leakage-remote-code-execution-and-many-more-104b09e644f4

RESEARCHER OF THE MONTH

Thank you, **@nzhg3i_nzm**, for exposing the serious vulnerability of PII and CAC ID being accessible on an unauthenticated page. This kind of oversight opens the door to identity theft, unauthorized access, and privacy breaches. Your vigilance is critical! **#DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking**

TOP VULNERABILITIES SINCE LAUNCH

81 CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES

35 CWE-200 INFORMATION DISCLOSURE

31 CWE-601 OPEN REDIRECT