DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE MARCH 2025

DIB-VDP

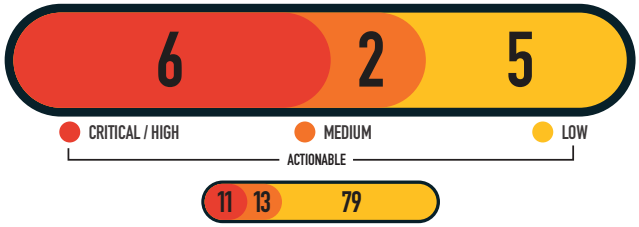
723
VULNERABILITIES SUBMITTED SINCE LAUNCH

26
VULNERABILITIES FOR THE MONTH

165
RESEARCHERS SINCE LAUNCH

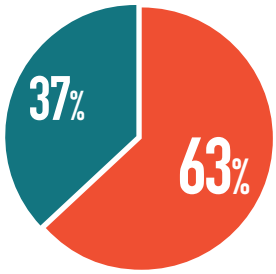
13
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



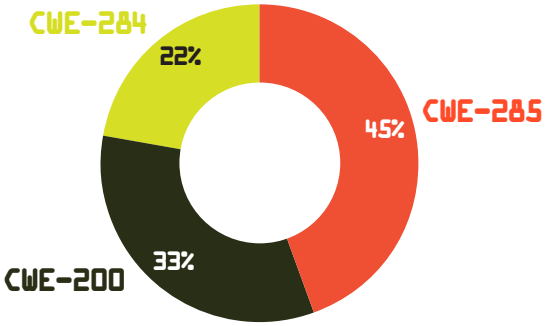
MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH



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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-285 IMPROPER AUTHORIZATION: 4
CWE-200 INFORMATION DISCLOSURE: 3
CWE-284 IMPROPER ACCESS CONTROL - GENERIC: 2

KNOWLEDGE BYTE

In March 2025, DIB-VDP received multiple reports describing a vulnerability related to response manipulation. Response manipulation involves intercepting a response sent from a server via a web client or attack proxy, altering the response, and posting the alterations back to the server. Exploits of this type could lead to potential authentication bypass, privilege escalation and sensitive data disclosure. Mitigations for this vulnerability can include input validation, output encoding, and implementing integrity checks on server responses.

Further information is available in the following resources:
https://owasp.org/www-project-top-ten/2017/A2_2017-Broken_Authentication
https://cwe.mitre.org/data/definitions/287.html

RESEARCHER OF THE MONTH

Shoutout to @Kaenne for their groundbreaking research on Authentication Bypass via Response Manipulation! This vulnerability poses a major threat to secure authentication—organizations must act fast to mitigate risks. Awareness is key! #DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH