DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE NOVEMBER 2024

DIB-VDP

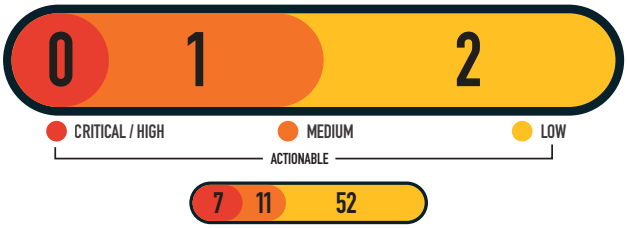
530
VULNERABILITIES SUBMITTED SINCE LAUNCH

13
VULNERABILITIES FOR THE MONTH

137
RESEARCHERS SINCE LAUNCH

3
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

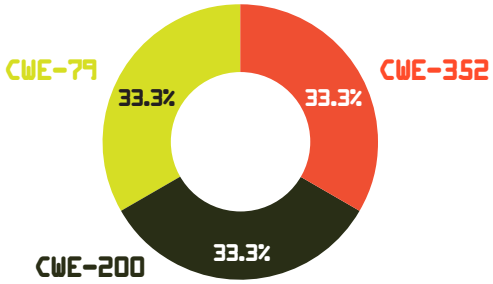


MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH

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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-352 CROSS-SITE REQUEST FORGERY (CSRF): 1
CWE-200 INFORMATION DISCLOSURE: 1
CWE- 79 CROSS-SITE SCRIPTING (XSS): 1

KNOWLEDGE BYTE

In November 2024, the DIB-VDP received a submission demonstrating a potential for a Cross-Site Request Forgery (CSRF) vulnerability. CSRF allows an attacker to force a user to submit a request without their consent. This attack has the potentional to allow an adversary the ability to send unintended messages from the victim that could be escalated to a phishing attack, unauthorized queries, or spam submissions on behalf of the victim. System owners are encouraged to preform one of the following: set appropriate cache-control headers, ensure that AJAX requests include the CSRF token in the request headers, and/or ensure that the CSRF token is refreshed when a new session is created. Further information is available in the following resources: https://owasp.org/www-community/attacks/csrf

https://cheatsheetseries.owasp.org/cheatsheets/Cross-Site_Request_Forgery_Prevention_Cheat_Sheet.html

RESEARCHER OF THE MONTH

Kudos to g_bi for discovered a critical XSS vulnerability. This highlights the importance of continuous security testing and vigilance. Stay safe out there! #DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH