DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE JANUARY 2025

DIB-VDP

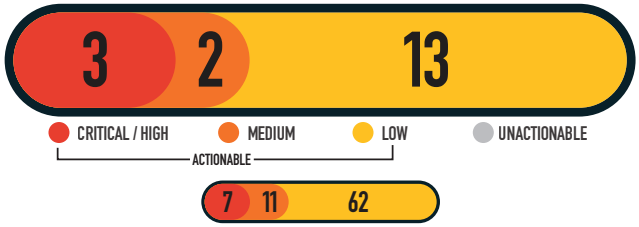
629
VULNERABILITIES SUBMITTED SINCE LAUNCH

80
VULNERABILITIES FOR THE MONTH

155
RESEARCHERS SINCE LAUNCH

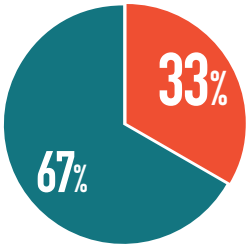
18
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



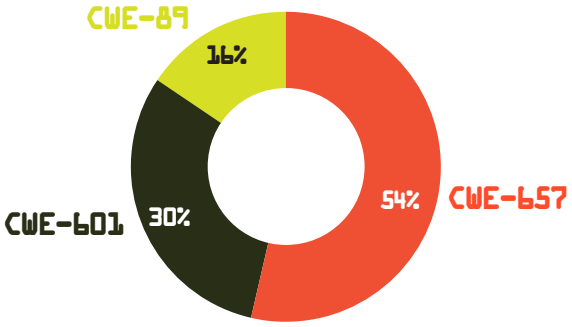
MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH



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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 7
CWE-601 OPEN REDIRECT: 4
CWE-89 SQL INJECTION: 2

KNOWLEDGE BYTE

In January 2025, the DIB-VDP received a submission demonstrating the potential for a JSON Web Token (JWT) Sensitivity Information Disclosure. The JWT allows an attacker to access sensitive data. The vulnerability occurs when an attacker alters the token and changes the hashing algorithm. This can lead to impersonating another user and bypassing authentication. The following is encouraged: add a user context in the token including random strings that will be generated during authentication, avoid setting explores header so that the cookies are cleared when the browser is closed, and set Max-Age to a value smaller or equal to the value of the JWT expiry. Further information is available in the following resources:

https://owasp.org/www-chapter-belgium/assets/2021/2021-02-18/JWT-Security.pdf

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

RESEARCHER OF THE MONTH

Huge thanks to @dox69 for uncovering the critical JWT info disclosure vulnerability! Your dedication to improving web security helps protect us all. This finding highlights the risks that could impact security frameworks. Stay vigilant! 🔐#DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

TOP VULNERABILITIES SINCE LAUNCH