DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE AUGUST 2024

DIB-VDP

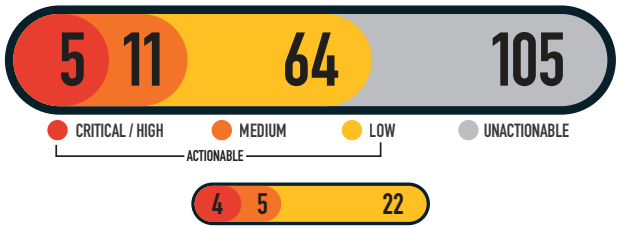
388
VULNERABILITIES SUBMITTED SINCE LAUNCH

185
VULNERABILITIES FOR THE MONTH

106
RESEARCHERS SINCE LAUNCH

80
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

100%

MITIGATIONS FOR THE MONTH

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

KNOWLEDGE BYTE

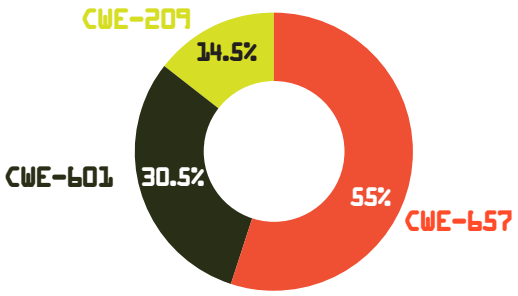
In August 2024, the DIB-VDP processed a report for a chained vulnerability involving Insecure Direct Object Reference (IDOR) to Stored Cross Site Scripting (XSS) that could potentially lead to an account takeover. IDOR is a type of access control vulnerability that arises when an application uses user-supplied input to access objects directly. A Stored XSS occurs when a malicious script is injected directly into a vulnerable web application. It is recommended to implement secure handling of all user inputs and implement access control checks for each object that users try to access. More information is available at:

https://nvd.nist.gov/vuln/detail/CVE-2023-30550
https://nvd.nist.gov/vuln/detail/CVE-2022-28599
https://cheatsheetseries.owasp.org/cheatsheets/Insecure_Direct_Object_Reference_Prevention_Cheat_Sheet.html

RESEARCHER OF THE MONTH

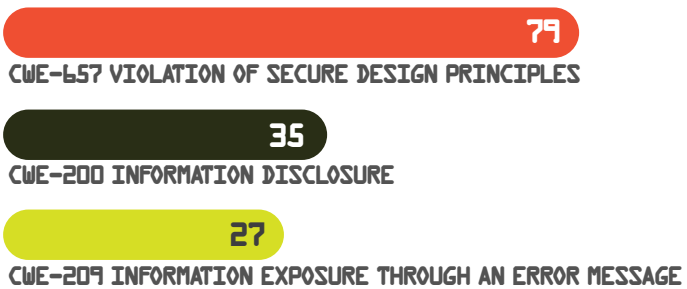
🚨 Security Breakthrough 🚨
Kudos to **Med Aziz Hassine** for discovering that chaining IDOR + Stored XSS can lead to full account takeover! 🛡️ Let's stay vigilant and secure our applications.
#DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking

VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH



CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 27
CWE-601 OPEN REDIRECT: 15
CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE: 7

TOP VULNERABILITIES SINCE LAUNCH



𝕏 @DC3VDP
AFOSI.DC3.DIB-VDP@us.af.mil

DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY