DOD DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM PILOT

MYTE BYTE NOVEMBER 2021

DIB-VDP

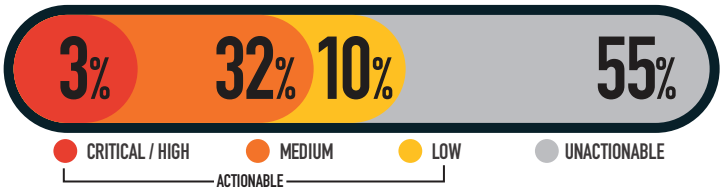
927 VULNERABILITIES SINCE LAUNCH

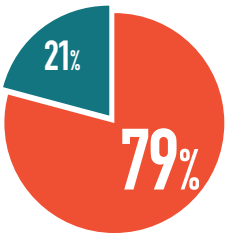
40 VULNERABILITIES FOR THE MONTH

244 RESEARCHERS SINCE LAUNCH

18 ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

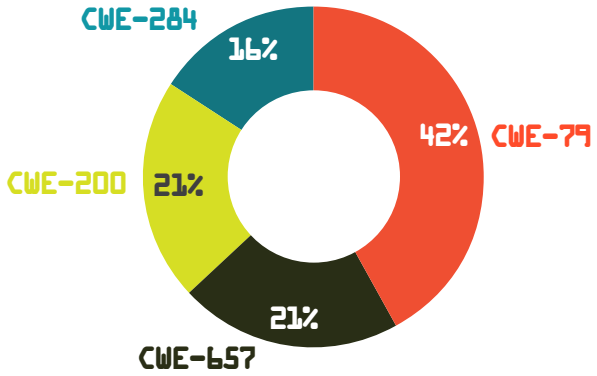




MITIGATIONS FOR THE MONTH

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

VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH



CWE-79 CROSS-SITE SCRIPTING (XSS): 8

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 4

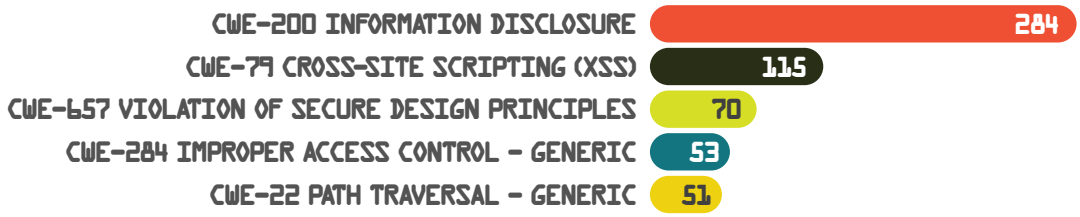
CWE-200 INFORMATION DISCLOSURE: 4

CWE-284 IMPROPER ACCESS CONTROL - GENERIC: 3

KNOWLEDGE BYTE

DIB-VDP received notification of an asset vulnerable to Reflected XSS via an email POST parameter in the sites registration page. XSS is a modification that occurs when user input is insecurely incorporated into HTML markup within a web page. When it does not escape properly, an attacker can inject malicious JavaScript which, once evaluated, can activate to show authenticated sessions and rewrite the design and functionality of the vulnerable page. The impact of a successful XSS exploitation varies. In a worst-case scenario, an attacker is able to execute JavaScript code within the victim's browser. This opens the door to many scenarios of which the most common are Session Hijacking, Client-Side Attacks, or redirecting users to a malicious site. System owners are encouraged to filter all user input on arrival, encode server data on output, use appropriate response headers that aren't intended to contain any HTML or JavaScript and to use a Content Security Policy (CSP) to reduce the severity of any XSS vulnerabilities that may still occur. Further reading on the impact of XSS attacks can be found at the link below:
https://csrc.nist.gov/glossary/term/cross_site_scripting

TOP VULNERABILITIES SINCE LAUNCH



@DC3VDP
AFOSI.DC3.DIB-VDP@us.af.mil

DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY