DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES MARCH 2025

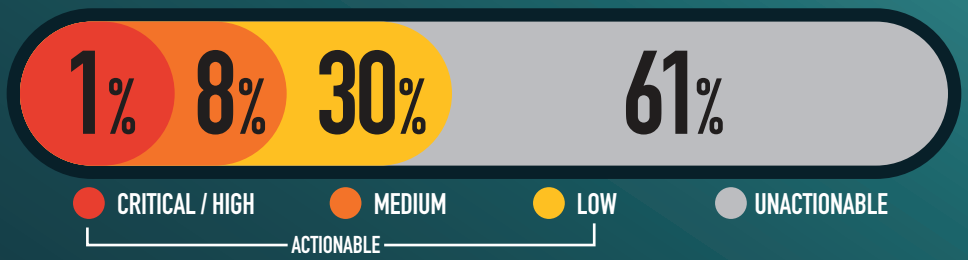
55,275
VULNERABILITIES SINCE LAUNCH

7,264
RESEARCHERS SINCE LAUNCH

30,079
ACTIONABLE REPORTS PROCESSED

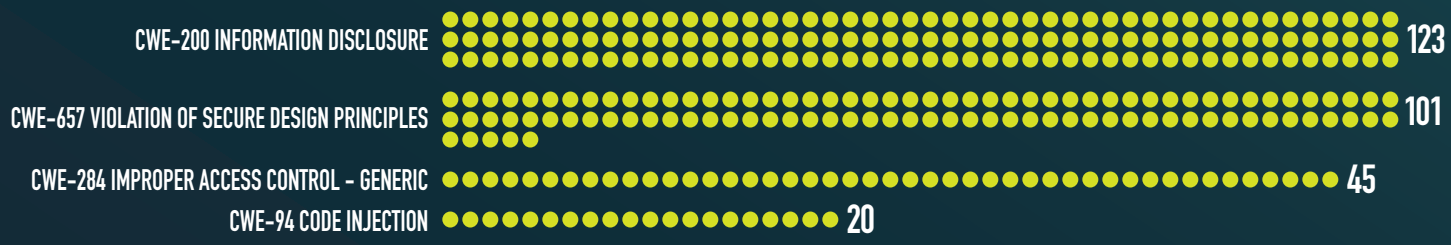
215
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In March 2025, the DoD VDP received a high severity submission identifying misconfigured access controls which could result in the disclosure of unauthorized information. Researchers identified a security flaw in a DoD web application that potentially allowed access to other user account profiles through modified web requests. It is recommended all system owners regularly evaluate the authorization workflows and role permissions used in their web applications to ensure sensitive data is protected. Further information is available in the following resources: https://portswigger.net/web-security/access-control & https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html & https://www.spiceworks.com/it-security/vulnerability-management/articles/insecure-direct-object-reference-idor

RESEARCHER OF THE MONTH

Sensitive data in plain sight–until **@j0nasdias** stepped in. Their discovery of an exposed debug file with database credentials earned them **March 2025 Researcher of the Month**.
Thanks for keeping our systems safe!
#CyberSecurity #DoDSecurity #InfoSec

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER