DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES SEPTEMBER 2025

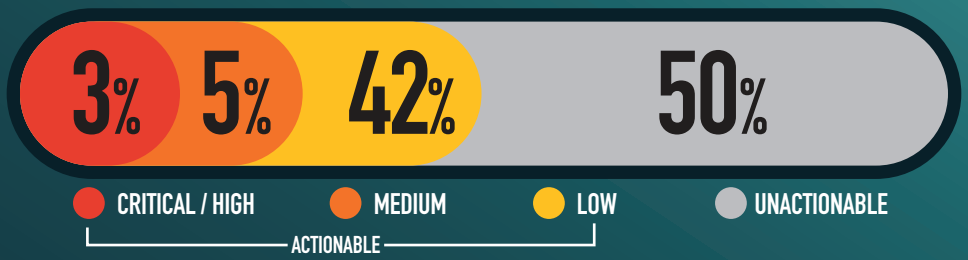
57,411
VULNERABILITIES SINCE LAUNCH

7,696
RESEARCHERS SINCE LAUNCH

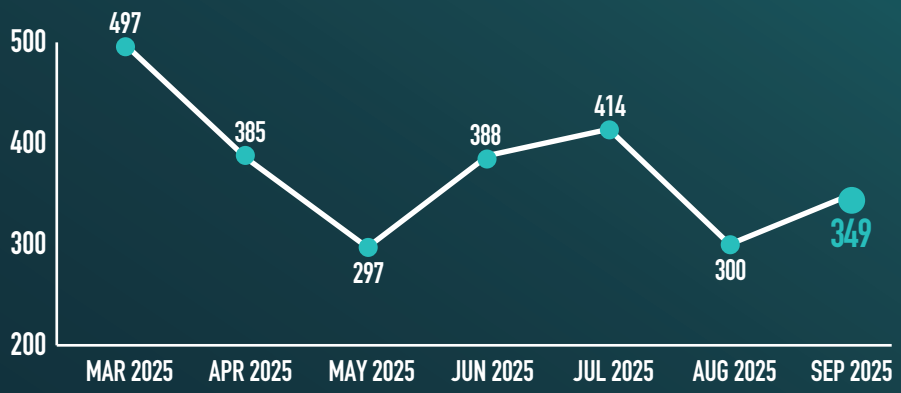
31,103
ACTIONABLE REPORTS PROCESSED

180
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE	84
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	69
CWE-312 CLEARTEXT STORAGE OF SENSITIVE INFORMATION	37
CWE-284: IMPROPER ACCESS CONTROL - GENERIC	25
CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE	24

KNOWLEDGE BYTE

In September 2025, the DoD VDP received a critical severity submission identifying a broken access control allowing for unauthorized modification of user accounts within a DoD web application. The unauthorized changes included the ability to trigger a password reset of the account. By intercepting the token granted by the reset password function, researchers demonstrated the potential to take control of a victim's account. It is recommended that system owners regularly review access controls of their web applications and implement best practices. Further information is available in the following resources: https://cheatsheetseries.owasp.org/cheatsheets/Authorization_Cheat_Sheet.html & https://portswigger.net/web-security/access-control & https://cheatsheetseries.owasp.org/cheatsheets/Forgot_Password_Cheat_Sheet.html

RESEARCHER OF THE MONTH

🚨Congrats to our *Researcher of the Month* for the DoD Vulnerability Disclosure Program: @Ahmed78752911!👏Selected for responsibly disclosing an IDOR vulnerability that enabled account takeover–a critical find that helps keep systems safer. **#DoDVulnerabilityDisclosure #CyberSecurity #BugBounty**

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER