DOD VULNERABILITY DISCLOSURE PROGRAM

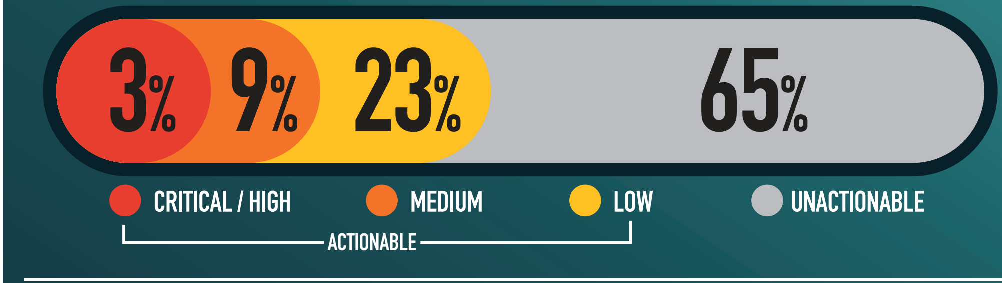
BUG BYTES MAY 2024

51,061
VULNERABILITIES SINCE LAUNCH

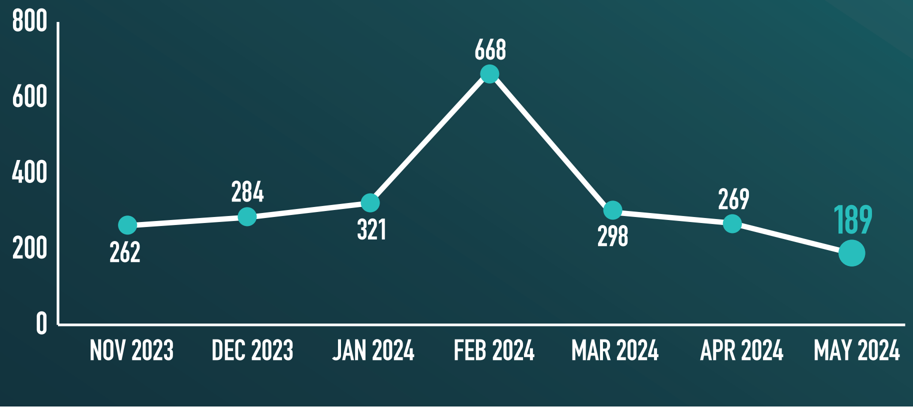
6,221
RESEARCHERS SINCE LAUNCH

28,501
ACTIONABLE REPORTS PROCESSED

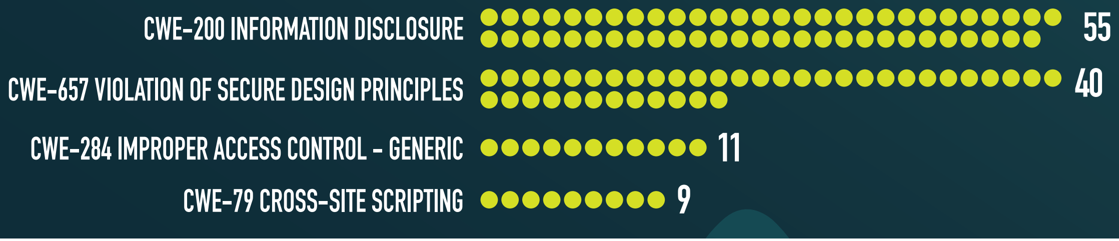
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In May 2024, the DoD VDP received a critical severity submission detailing the potential to take over a Department of Defense subdomain. Domain and subdomain takeovers typically occur as services are decommissioned or migrated to a new host and corresponding Domain Name Service (DNS) records are not updated. Outdated DNS records may result in traffic going to a third-party host that is not DoD controlled. This month, researchers identified an outdated DNS record and corresponding host that could be used to provide unauthorized third-party content. System owners should routinely monitor their attack surface and ensure all DNS records are current. Further information is available in the following resources: https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/02-Configuration_and_Deployment_Management_Testing/10-Test_for_Subdomain_Takeover & https://www.hackerone.com/hackerone-community-blog/guide-subdomain-takeovers & https://kevin.borgolte.me/files/pdf/ndss2018-cloud-strife.pdf

RESEARCHER OF THE MONTH

🚨 Important Discovery! 🚨 @martinvw has identified a critical security gap: a subdomain pointing to an unregistered domain! This flaw can let attackers host malicious content, intercept emails, execute XSS attacks, steal cookies, and trick password managers.

Be sure to check your domain configurations to prevent these threats! #Cybersecurity #Infosec #DODVDP

X @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3
DOD CYBER CRIME CENTER