DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES MAY 2025

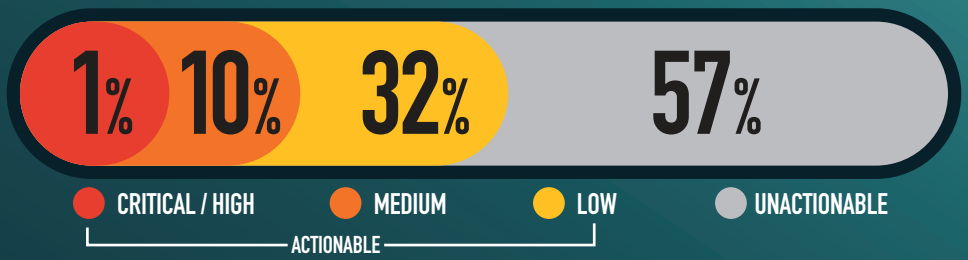
55,958
VULNERABILITIES SINCE LAUNCH

7,424
RESEARCHERS SINCE LAUNCH

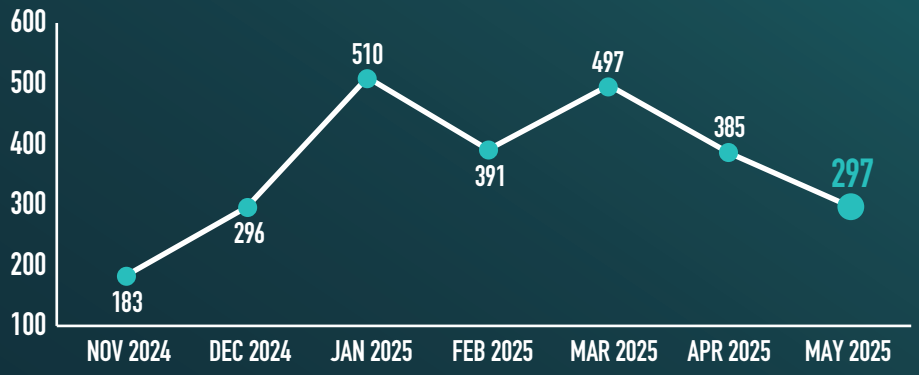
30,384
ACTIONABLE REPORTS PROCESSED

137
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	57
CWE-200 INFORMATION DISCLOSURE	56
CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE	29
CWE-79 CROSS-SITE SCRIPTING	27
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	17

KNOWLEDGE BYTE

In May 2025, several high severity submissions were received by the DoD VDP demonstrating possible SQL injections (SQLi). Researchers identified multiple parameters used by backend databases that accepted unfiltered input. Crafting specific payloads to target the database management systems could result in data exfiltration, system downtime, or data manipulation. All parameters and queries should utilize appropriate input validation and follow safe coding practices. Further information can be found in the following resources: https://portswigger.net/web-security/sql-injection & https://cheatsheetseries.owasp.org/cheatsheets/SQL_Injection_Prevention_Cheat_Sheet.html & https://sites.cc.gatech.edu/fac/Alex.Orso/papers/halfond.viegas.orso.ISSSE06.pdf

RESEARCHER OF THE MONTH

Big thanks to reinhardtthe for exposing the dangers of reflected cross-site scripting! 🚨 A misconfiguration like this can lead to widespread data theft and serious security breaches. Always properly secure Web Application Firewalls! 🔐**#CyberSecurity #InfoSec #WebSecurity #DataProtection**

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER