DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES JANUARY 2025

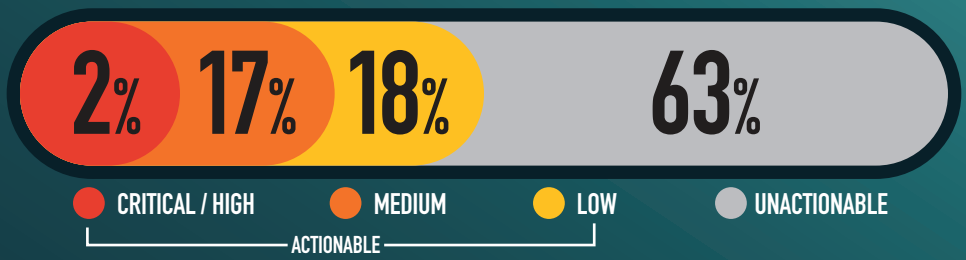
54,386
VULNERABILITIES SINCE LAUNCH

7,084
RESEARCHERS SINCE LAUNCH

29,776
ACTIONABLE REPORTS PROCESSED

220
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE	186
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	102
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	69
CWE-79 CROSS-SITE SCRIPTING	17

KNOWLEDGE BYTE

In January 2025, the DoD VDP received a critical severity submission with the potential for unauthorized data modification through GraphQL queries. GraphQL is a query language and runtime that provides clients with tools to interact with API datasets. Researchers identified a misconfiguration allowing them to map the API service. With detailed knowledge of the service, it may be possible to locate sensitive data or gain write permissions to restricted data. System owners are encouraged to review GraphQL and other API endpoints to verify all permissions follow security best practices. Further information is available in the following resources:
https://www.apollographql.com/docs/graphos/platform/security/overview
https://portswigger.net/web-security/graphql
https://cheatsheetseries.owasp.org/cheatsheets/GraphQL_Cheat_Sheet.html

RESEARCHER OF THE MONTH

Hats off to **Jared Hrabak (@badlifeguard)** for his game-changing discovery–a flaw in an internal system that risked exposing military members' sensitive information. Your proactive work helps keep our heroes safe. We appreciate your relentless pursuit of security! **#CyberSecurity #DoDSecurity #InfoSec**

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER