DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES MARCH 2026

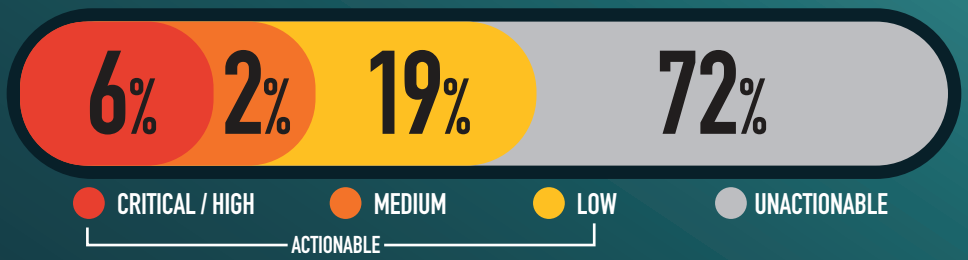
59,310
VULNERABILITIES SINCE LAUNCH

5,681
RESEARCHERS SINCE LAUNCH

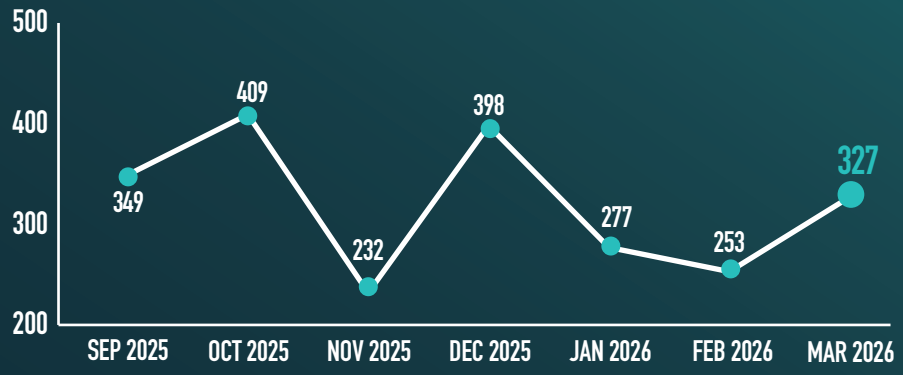
31,926
ACTIONABLE REPORTS PROCESSED

108
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATIONS FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE	74
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	54
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	19
CWE-79 CROSS-SITE SCRIPTING	9
CWE-287 IMPROPER AUTHENTICATION - GENERIC	8

KNOWLEDGE BYTE

In March 2026, the DoD VDP received a critical severity submission utilizing an access control vulnerability to gain full access to hosted content. Researchers identified a broken access control that led to the capture of authentication tokens within the Strapi CMS framework. The captured tokens allowed for control to create, read, upload, and delete content within the site. It is recommended that system owners regularly review the authentication flow of systems to limit the potential for token interception. Further information is available in the following resources:

https://portswigger.net/web-security/jwt

https://portswigger.net/web-security/authentication/securing

https://cheatsheetseries.owasp.org/cheatsheets/JSON_Web_Token_for_Java_Cheat_Sheet.html

RESEARCHER OF THE MONTH

Huge congratulations to @Daniel_Farinax for being named Researcher of the Month. They are being recognized for finding a way to obtain unauthenticated CRUD access to DoD training articles. This vulnerability was made possible through use of an open user registration API. Well deserved! **#CyberSecurity #VDP**

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER