DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES JANUARY 2026

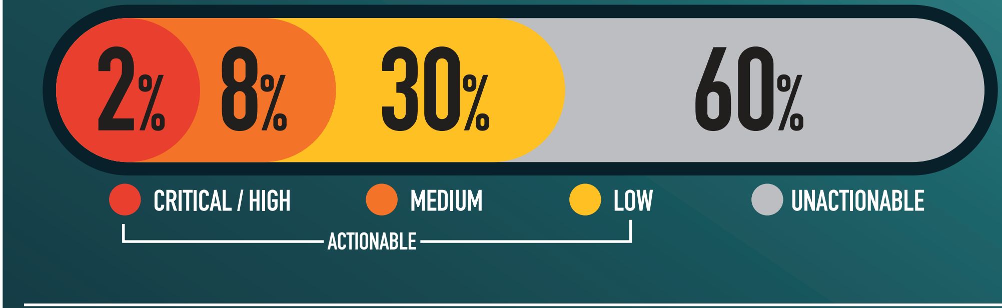
58,728
VULNERABILITIES SINCE LAUNCH

8,010
RESEARCHERS SINCE LAUNCH

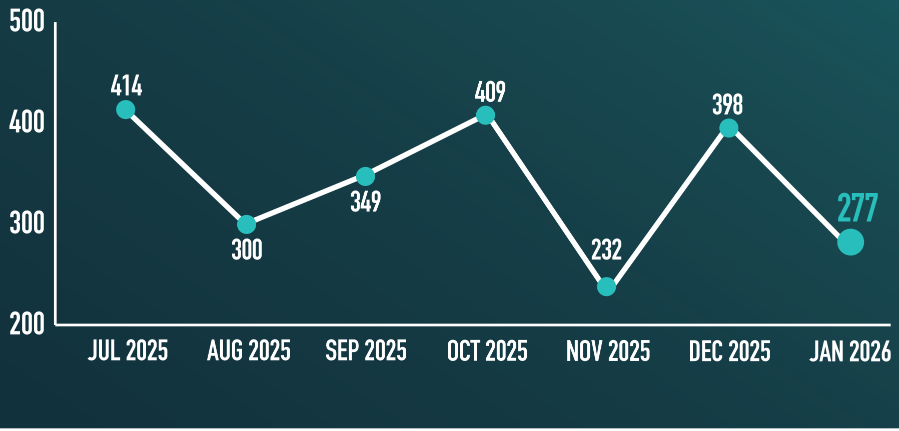
31,720
ACTIONABLE REPORTS PROCESSED

116
ACTIONABLE VDPS FOR THE MONTH

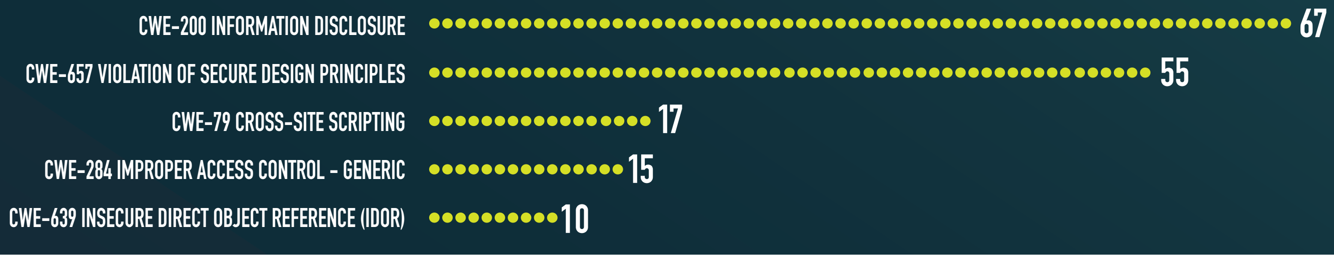
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In January 2026, the DoD VDP received a critical severity submission that could grant unauthorized users access to sensitive information. Researchers identified a permission issue that would allow for the retrieval of unauthorized files with a known file identifier. The use of sequential values for file identifiers could lead to the enumeration of multiple system files. It is recommended that all system owners regularly review access control permissions and utilize appropriate randomization for sensitive identifiers. Further information is available in the following resources:

https://portswigger.net/web-security/access-control

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

RESEARCHER OF THE MONTH

Big shoutout to @ItsKenshin04 for snagging Researcher of the Month with the DoD Vulnerability Disclosure Program! @ItsKenshin04 found an IDOR vulnerability which allowed them to view and download vast quantities of sensitive PII, such as finance related details, in connection to military personnel. 📄🤑 **#VDP #BugBounty #Cybersecurity**

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3
DOD CYBER CRIME CENTER