DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES NOVEMBER 2024

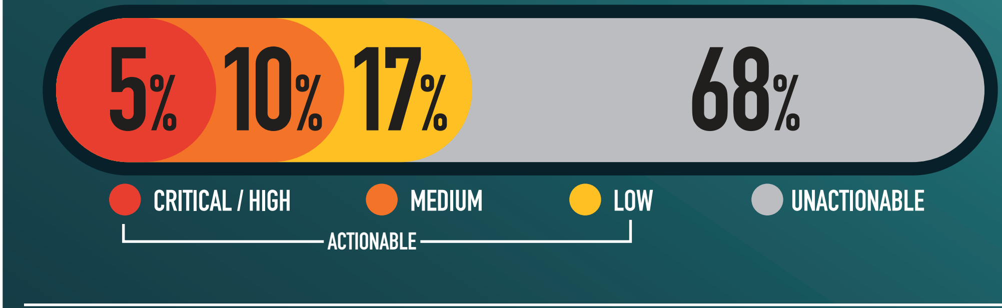
53,576
VULNERABILITIES SINCE LAUNCH

6,914
RESEARCHERS SINCE LAUNCH

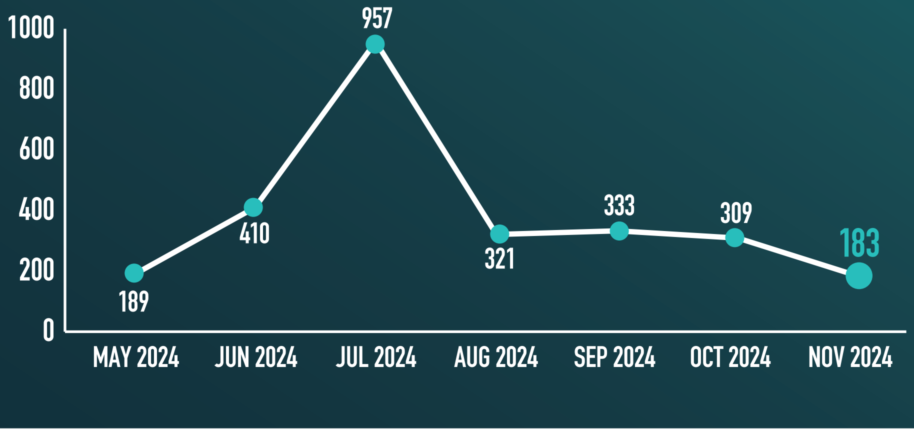
29,448
ACTIONABLE REPORTS PROCESSED

63
ACTIONABLE VDPS FOR THE MONTH

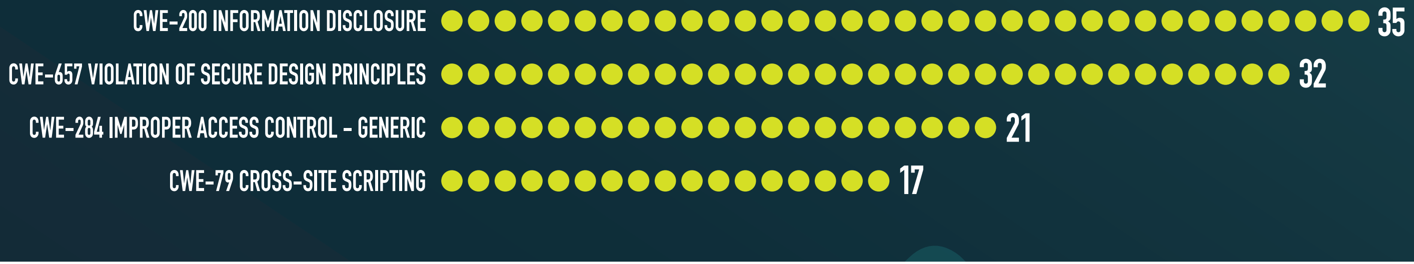
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In November 2024, the DoD VDP received a critical severity submission detailing the presence of hardcoded credentials in multiple public files. Researchers located publicly stored backups and JavaScript configuration files containing various credential sets. The credentials, if valid, could allow access to systems, including SMTP servers, AWS instances, or system databases. System owners are encouraged to review all public assets, restrict access to sensitive credentials, and regularly rotate secret keys. Further information is available in the following resources: https://cheatsheetseries.owasp.org/cheatsheets/Secrets_Management_Cheat_Sheet.html & https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_finding-unused.html & https://arxiv.org/pdf/2208.11280

RESEARCHER OF THE MONTH

Sensitive information was discovered in an exposed zip file, thanks to the sharp-eyed efforts of **Kyan Macdonald (@0xKMac)** and their team. This finding reinforces the need for robust file storage security. Great work, Kyan! #CyberSecurity #InfoSec #DoDSecurity

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3
DOD CYBER CRIME CENTER