DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES FEBRUARY 2026

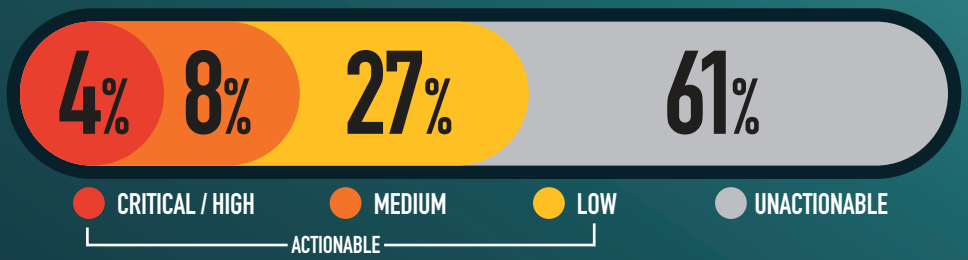
58,981
VULNERABILITIES SINCE LAUNCH

5,607
RESEARCHERS SINCE LAUNCH

31,835
ACTIONABLE REPORTS PROCESSED

121
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES

LEADING COMMON WEAKNESS ENUMERATIONS FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE	98
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	38
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	10
CWE-312 CLEARTEXT STORAGE OF SENSITIVE INFORMATION	6
CWE-601 OPEN REDIRECT	6

KNOWLEDGE BYTE

In February 2026, the DoD VDP received a critical severity submission outlining the use of internet repositories to access PII and other sensitive information. Internet repositories, such as Wayback Machine or VirusTotal, can be used to capture point-in-time snapshots of public systems and files. Researchers were able to utilize these platforms to locate remnant database files that potentially contained PII and other sensitive information in clear text. It is recommended that all system owners regularly review the public footprint of their systems and ensure sensitive data is properly safeguarded. Further information is available in the following resources:

https://top10proactive.owasp.org/archive/2018/c8-protect-data-everywhere/

https://portswigger.net/web-security/information-disclosure

https://arxiv.org/pdf/2602.21826

RESEARCHER OF THE MONTH

Huge congratulations to @janssonm for being named Researcher of the Month. They are being recognized for finding a way to achieve privilege escalation on the target website via use of an exposed email verification token. Well deserved! 🔥💻 #Cybersecurity #VDP

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER