DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES APRIL 2025

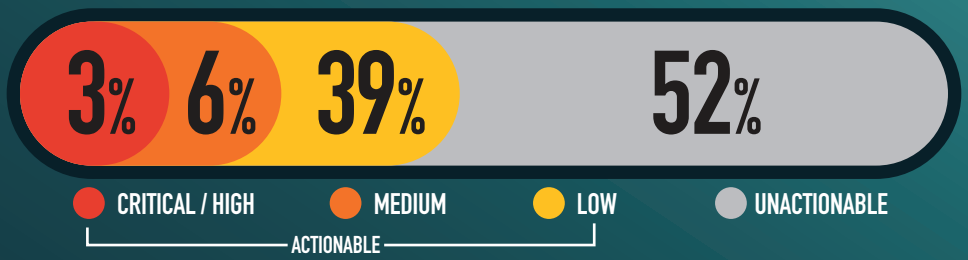
55,661
VULNERABILITIES SINCE LAUNCH

7,344
RESEARCHERS SINCE LAUNCH

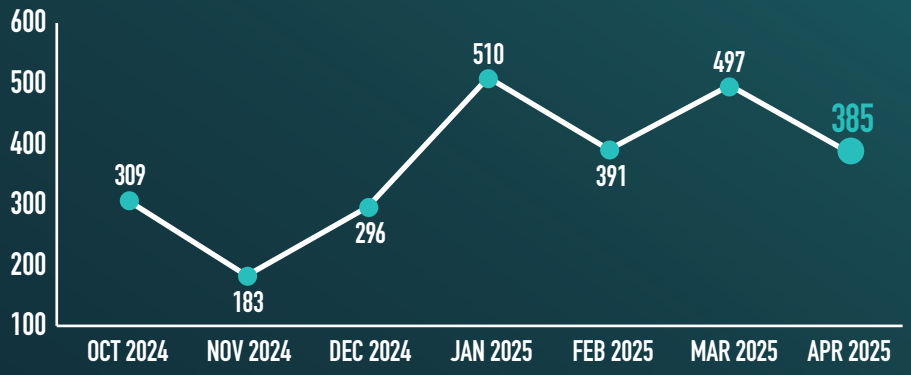
30,255
ACTIONABLE REPORTS PROCESSED

187
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

KNOWLEDGE BYTE

In April 2025, the DoD VDP received a high severity submission identifying the possibility of bypassing authentication within specific versions of PAN-OS and accessing web management functions. PAN-OS is software used to control and manage Palo Alto firewalls. Researchers identified an encoding flaw that allowed specially crafted payloads to access unauthorized functions of PAN-OS. The payloads may be capable of running customized scripts or resetting the firewall settings to a default state. It is recommended all system owners update to the latest approved version of PAN-OS. Further information is available in the following resources: https://security.paloaltonetworks.com/CVE-2025-0108 & https://nvd.nist.gov/vuln/detail/cve-2025-0108 & https://www.assetnote.io/resources/research/nginx-apache-path-confusion-to-auth-bypass-in-pan-os

RESEARCHER OF THE MONTH

@mv_rakie earns ROTM for identifying a misconfigured API endpoint leaking PII—names, emails, roles, and auth data. This impactful discovery helps drive stronger protections across DoD systems. Thank you for your outstanding work! **#CyberSecurity #DoDSecurity #InfoSec**

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER