DOD VULNERABILITY DISCLOSURE PROGRAM

BUG BYTES APRIL 2024

50,871

VULNERABILITIES SINCE LAUNCH

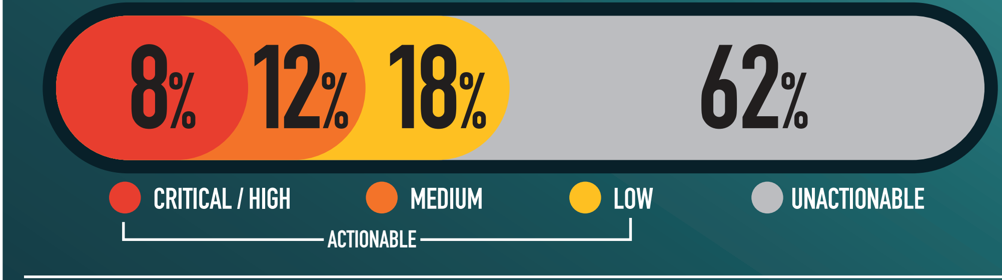
6,157

RESEARCHERS SINCE LAUNCH

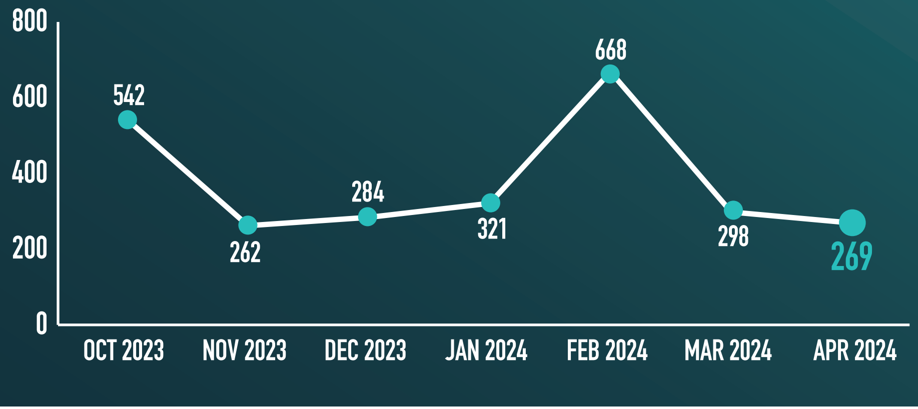
28,434

ACTIONABLE REPORTS PROCESSED

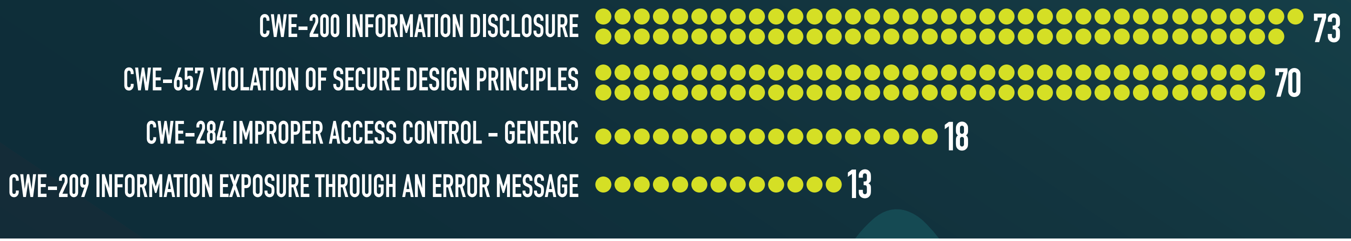
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In April 2024, the DoD VDP received several critical severity submissions detailing potential remote code execution within Palo Alto firewalls utilizing specific versions of PAN-OS. CVE-2024-3400 details a vulnerability in this software used to run Palo Alto firewalls, where the operating system could inject and read custom session values. The modified session values could allow the firewall to communicate with third-party servers and execute code. Researchers located several Palo Alto endpoints that were potentially susceptible to this vulnerability. It is recommended that all system owners with Palo Alto firewalls running affected PAN-OS versions update to the latest release versions and continue to monitor network traffic for abnormalities. Further information is available in the following resources: https://security.paloaltonetworks.com/CVE-2024-3400

https://www.paloaltonetworks.com/blog/2024/04/more-on-the-pan-os-cve/

https://iavm.csd.disa.mil/iavm-notice-html/145913

RESEARCHER OF THE MONTH

🛡️ Stay ahead of cyber threats! **@gi7w0rm's** latest report highlights a critical vulnerability in Palo Alto Networks PAN-OS software, emphasizing the importance of robust cybersecurity measures. Stay informed and secure your systems! #CybersecurityAwareness #DODVDP

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3
DOD CYBER CRIME CENTER