DOD VULNERABILITY DISCLOSURE PROGRAM

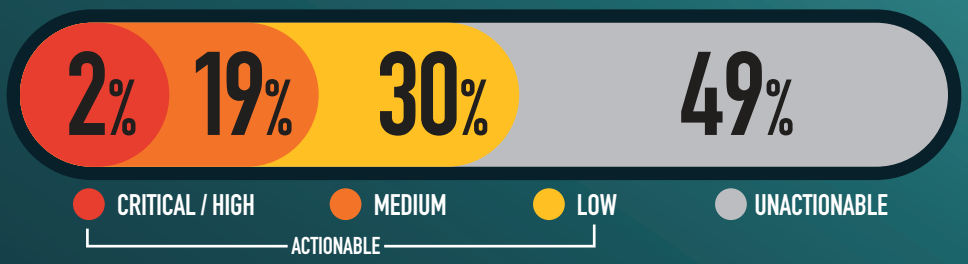
BUG BYTES MARCH 2023

46,261
VULNERABILITIES SINCE LAUNCH

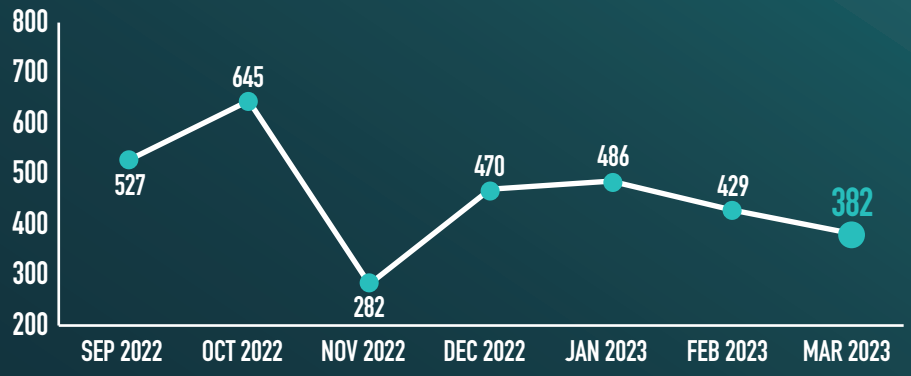
4,753
RESEARCHERS SINCE LAUNCH

26,487
ACTIONABLE REPORTS PROCESSED

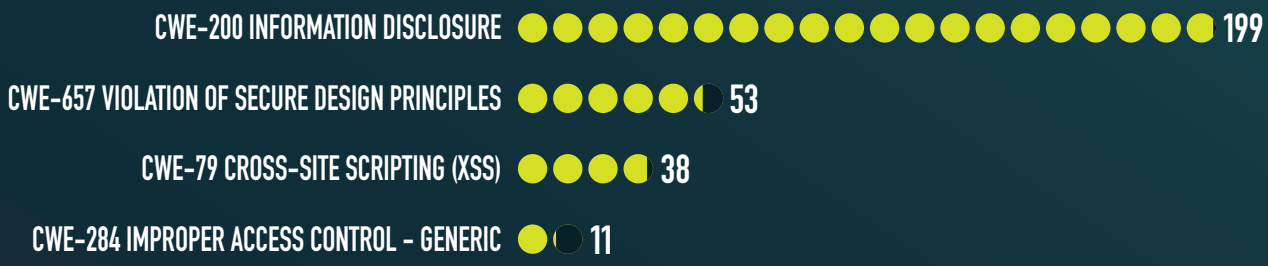
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In March 2023, the DoD VDP received multiple critical submissions displaying denial of service attacks against sites hosting WordPress installations. Researchers were able to exploit a publicly accessible webpage within WordPress that caused the server to load all active modules. By repeatedly requesting the webpage, researchers were able to exhaust the resources of the webhost and impact availability of services on the site. It is recommended for system owners to ensure proper hardening measures for WordPress are being followed for their environment. See the following for more information:
https://nvd.nist.gov/vuln/detail/CVE-2018-6389
https://wordpress.org/documentation/article/hardening-wordpress/
https://thehackernews.com/2018/02/wordpress-dos-exploit.html

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for March 2023 is @0rionh4ck! They submitted several critical reports including sensitive data disclosure and blind server-side request forgery on a DOD asset; if not remediated would lead to unauthorized actions on DOD servers or access to sensitive information. Thank you very much! VDP Hackers for the win!

@DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER