



46,261

4,753

26,487

ACTIONABLE REPORTS PROCESSED

Risk Level	Percentage
CRITICAL / HIGH	2%
MEDIUM	19%
LOW	30%
UNACTIONABLE	49%

ACTIONABLE (includes Critical/High, Medium, and Low risk levels)

Month	Confirmed COVID-19 cases
SEP 2022	527
OCT 2022	645
NOV 2022	282
DEC 2022	470
JAN 2023	486
FEB 2023	429
MAR 2023	382

CWE-200 INFORMATION DISCLOSURE ●●●●●●●●●●●●●●●●●●●● 199

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●●●● 53

CWE-79 CROSS-SITE SCRIPTING (XSS) ●●●● 38

CWE-284 IMPROPER ACCESS CONTROL - GENERIC ●● 11

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>

The DoD VDP Researcher of the Month for March 2023 is [@Orianh4ck](#)! 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!