DOD VULNERABILITY DISCLOSURE PROGRAM

FEBRUARY 2023

800

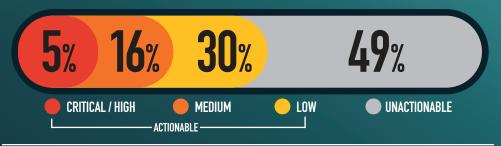


VULNERABILITIES SINCE LAUNCH

RESEARCHERS SINCE LAUNCH

26.3° **ACTIONABLE REPORTS PROCESSED**

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES 486



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-79 CROSS-SITE SCRIPTING (XSS) 31

CWE-400 DENIAL OF SERVICE 21

KNOWLEDGE BYTE

In February 2023, the DoD VDP received a critical submission regarding verbose error messaging, allowing a researcher to extract PII from a government system. The researcher was able to exploit a password recovery feature found on the website to successfully enumerate valid Social Security Numbers (SSNs) of government personnel. By entering crafted data into the password recovery form the website would return a message indicating that a SSN existed or did not exist in the current database allowing the researcher to compile a list of active SSNs from the site. It is important that system owners ensure authentication messages do not reveal any information that is not required to unauthorized personnel. See the following for more information:

https://cwe.mitre.org/data/definitions/204.html

https://cheatsheetseries.owasp.org/cheatsheets/Authentication Cheat Sheet.html https://portswigger.net/web-security/authentication/securing

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for February 2023 is @7v43t! They submitted a critical report of an improper error message producing sensitive information on a DoD asset; if not remediated, it would have led to credential harvesting. Thank you very much! VDP Hackers for the win!



