DOD VULNERABILITY DISCLOSURE PROGRAM

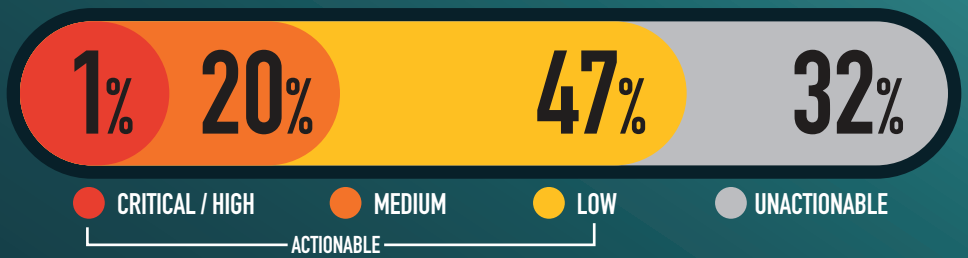
BUG BYTES DECEMBER 2022

44,921
VULNERABILITIES SINCE LAUNCH

3,866
RESEARCHERS SINCE LAUNCH

25,863
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE	108
CWE-79 CROSS-SITE SCRIPTING (XSS)	107
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	89
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	85

KNOWLEDGE BYTE

In December 2022, a researcher was able to provide a proof of concept exploiting default security credentials within an ESRI platform, gaining administrative rights. This allowed them to edit, upload, and delete data pertaining to the hosted GeoPortal projects. It is recommended that system owners evaluate their applications and public facing assets to ensure all accounts are appropriately hardened. See the following for more information:
https://www.stigviewer.com/stig/application_security_and_development/2020-09-30/finding/V-222662
https://www.stigviewer.com/stig/application_security_and_development/2020-09-30/finding/V-222661
https://owasp.org/Top10/A07_2021-Identification_and_Authentication_Failures/

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for December 2022 is **@CDH**! They submitted a critical report for a subdomain takeover on a DoD asset that could lead to an attacker gaining control of a targeted domain. Thank you very much! VDP Hackers for the win!

@DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER