DOD VULNERABILITY DISCLOSURE PROGRAM
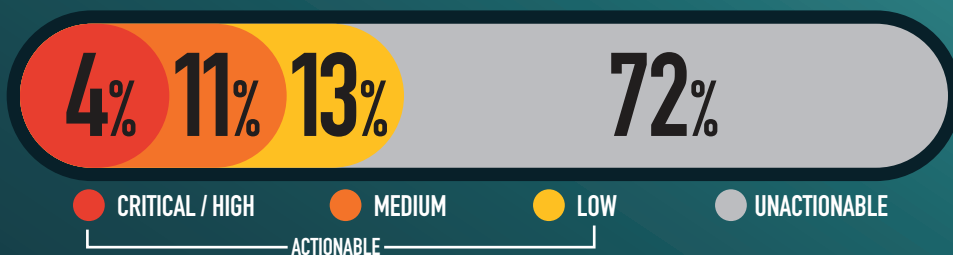# BUG BYTES APRIL 2023

46,584
VULNERABILITIES SINCE LAUNCH

4,795
RESEARCHERS SINCE LAUNCH

26,567
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

4% **11%** **13%** **72%**

● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE
ACTIONABLE

SUBMITTED VULNERABILITIES

Month	Value
OCT 2022	645
NOV 2022	282
DEC 2022	470
JAN 2023	486
FEB 2023	429
MAR 2023	382
APR 2023	323

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE ●●●●●●●●◐ 84

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●●●●◐ 64

CWE-79 CROSS-SITE SCRIPTING (XSS) ●●● 30

CWE-296 IMPROPER FOLLOWING OF A CERTIFICATE'S CHAIN OF TRUST ●●◐ 27

KNOWLEDGE BYTE

In April 2023, the DoD VDP received a critical submission allowing a researcher to obtain access tokens used within an Amazon Web Services, AWS, environment. The researcher was able to leverage features within the environment to bypass security measures and forge requests on behalf of the internal servers. These requests allowed them to exfiltrate sensitive details regarding the configuration, access tokens, and other AWS metadata. It is recommended that system owners follow best practices to safeguard instance metadata and limit IAM permission within their environment. See the following for more information: https://aws.amazon.com/blogs/security/defense-in-depth-open-firewalls-reverse-proxies-ssrf-vulnerabilities-ec2-instance-metadata-service/ & https://aws.amazon.com/iam/resources/best-practices/ & https://cheatsheetseries.owasp.org/cheatsheets/Server_Side_Request_Forgery_Prevention_Cheat_Sheet.html

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for April 2023 is **@basu_banakar**! They submitted a critical report for server-side request forgery on a DOD asset; that if not remediated would lead to unauthorized actions on DOD server. Thank you very much! VDP Hackers for the win!