DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES OCTOBER 2022
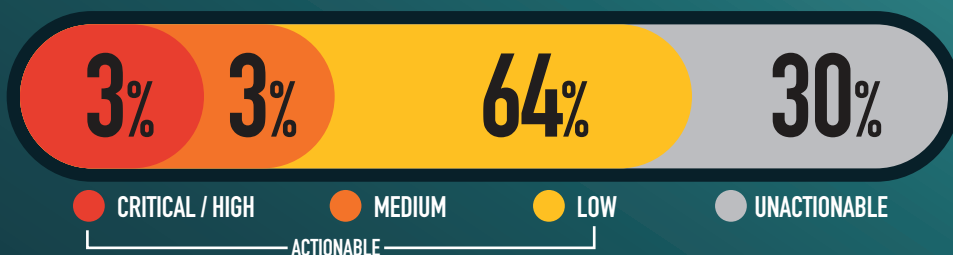
43,921
VULNERABILITIES SINCE LAUNCH

3,795
RESEARCHERS SINCE LAUNCH

25,232
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

3%	3%	64%	30%
CRITICAL / HIGH	MEDIUM	LOW	UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

	APR 2022	MAY 2022	JUN 2022	JUL 2022	AUG 2022	SEP 2022	OCT 2022
	446	359	252	1156	576	527	645

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●●●●●●●●●●●●●●●●●●●●●●● 250

CWE-284 IMPROPER ACCESS CONTROL - GENERIC ●●●●●●●●●●●●●◐ 137

CWE-200 INFORMATION DISCLOSURE ●●●●●●●●●◐ 102

CWE-79 CROSS-SITE SCRIPTING (XSS) ●●◐ 28
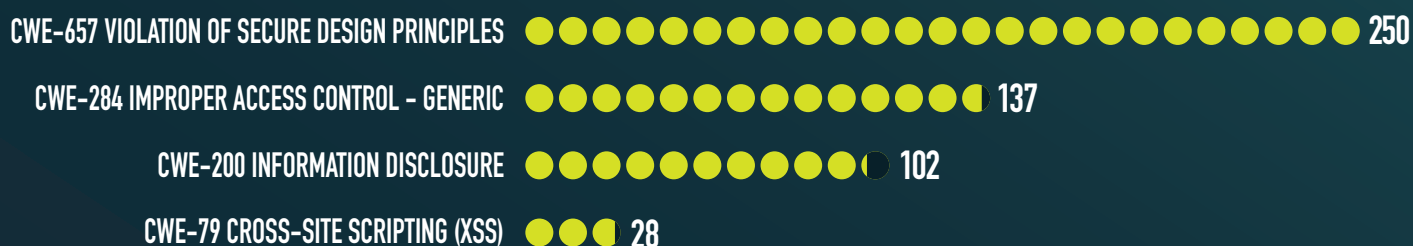
KNOWLEDGE BYTE

In October 2022, the DoD VDP received multiple high and critical severity findings where researchers were able to upload arbitrary files to DoD hosts without restriction. Uploading custom files can lead to many high impact attacks such as Denial of Service via resource exhaustion, credential theft, and command execution. Researchers were able to locate multiple endpoints with the PUT and DELETE methods enabled allowing for the upload and removal of files hosted on the server. As systems grow more complex, it is important for administrators and system owners to regularly audit all public facing endpoints to ensure only necessary HTTP methods are enabled. For further reading on the effects of unsecured file uploads and a full listing of all HTTP methods please see the following:
https://owasp.org/www-community/vulnerabilities/Unrestricted_File_Upload &
https://portswigger.net/web-security/file-upload & https://www.rfc-editor.org/rfc/rfc7231

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for October 2022 is @maliciousgroup! They submitted a critical report for unauthorized file uploads on a DoD asset; if not remediated would lead to malicious file execution. Thank you very much! VDP Hackers for the win!

@DC3VDP
DC3.VDPQuestions@us.af.mil

DC3
DOD CYBER CRIME CENTER