DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES MAY 2021
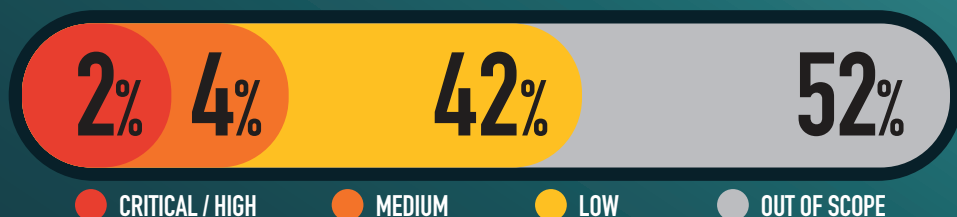
30,887
VULNERABILITIES SINCE LAUNCH
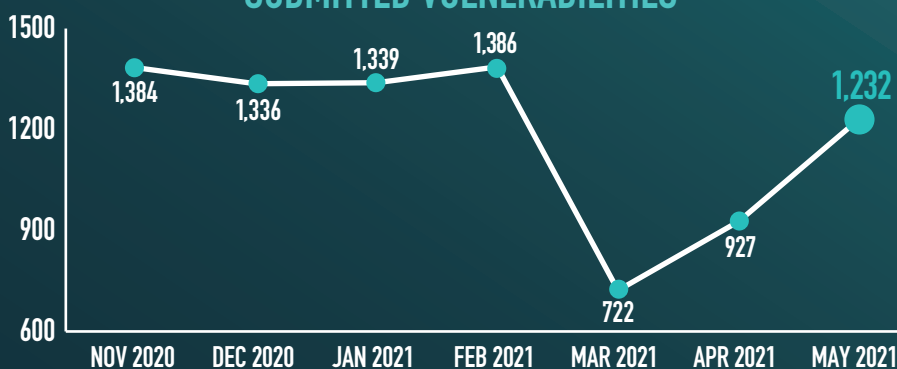
3,811
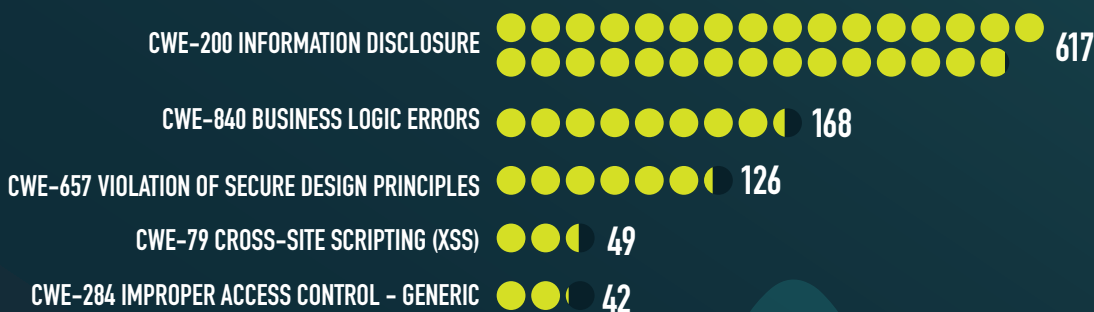RESEARCHERS SINCE LAUNCH

19,408
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

2% **4%** **42%** **52%**

● CRITICAL / HIGH ● MEDIUM ● LOW ● OUT OF SCOPE

SUBMITTED VULNERABILITIES

	NOV 2020	DEC 2020	JAN 2021	FEB 2021	MAR 2021	APR 2021	MAY 2021
	1,384	1,336	1,339	1,386	722	927	1,232

(Y-axis: 600, 900, 1200, 1500)

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE — 617

CWE-840 BUSINESS LOGIC ERRORS — 168

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 126

CWE-79 CROSS-SITE SCRIPTING (XSS) — 49

CWE-284 IMPROPER ACCESS CONTROL - GENERIC — 42

KNOWLEDGE BYTE

On 25 May VMware released a patch regarding two critical remote code execution flaws. The vulnerabilities affect VMware vCenter Server and VMware Cloud Foundation tracked as CVE-2021-21985 and CVE-2021-21986. CVE-2021-21985 allows attackers with access to port 443 the ability for commands with unrestricted privileges to be executed on the underlying operating system, whereas CVE-2021-21986 contains a vulnerability in a vSphere authentication mechanism. At this time, DODIN is not aware of any incidents affecting the DoD; however, VMware urged customers to patch affected servers immediately. Additional information regarding the CVEs and patches can be found at the following:
https://iavm.csd.disa.mil/iavm-notice-html/143566
https://www.vmware.com/security/advisories/VMSA-2021-0010.html

RESEARCHER OF THE MONTH

We are excited to announce the May 2021 DoD VDP Researcher of the Month Award goes to Lance Cleghorn with Defense Digital Services. As our first ever two-time researcher of the month winner, who submitted 4 Server-Side Request Forgery (SSRF) reports last month with multiple bypassing NIPR only access! Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program! Happy Hacking!

🐦 @DC3VDP
VDP-Questions@DC3.mil

DC3 DOD CYBER CRIME CENTER