DOD VULNERABILITY DISCLOSURE PROGRAM
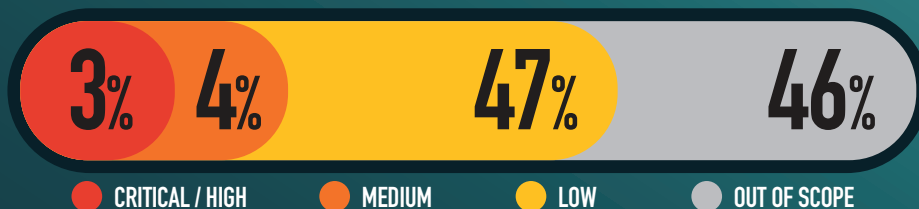# BUG BYTES FEBRUARY 2021

28,003
VULNERABILITIES SINCE LAUNCH

2,353
RESEARCHERS SINCE LAUNCH
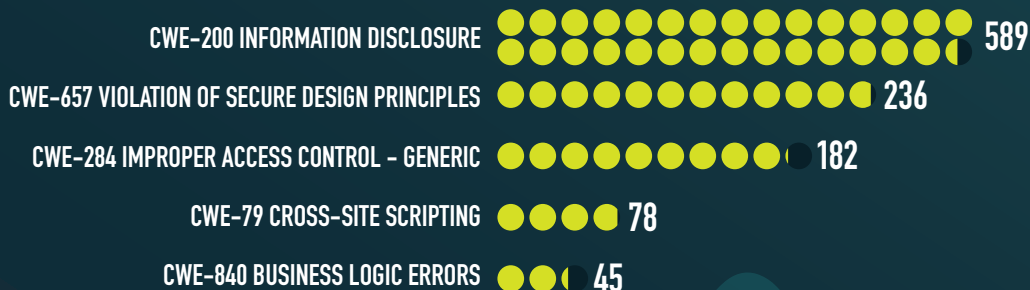
18,053
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

3% **4%** **47%** **46%**

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

SUBMITTED VULNERABILITIES

	AUG 2020	SEP 2020	OCT 2020	NOV 2020	DEC 2020	JAN 2021	FEB 2021
	1,203	1,143	2,176	1,384	1,336	1,339	1,386

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE — 589

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 236

CWE-284 IMPROPER ACCESS CONTROL – GENERIC — 182

CWE-79 CROSS-SITE SCRIPTING — 78

CWE-840 BUSINESS LOGIC ERRORS — 45

KNOWLEDGE BYTE

The DoD VDP recently received multiple submissions highlighting CVE-2021-26855; a Microsoft Exchange remote code execution vulnerability. This vulnerability is actively being exploited in the wild to allow attackers access to email inbox content and the ability to move laterally within systems. According to OSINT reporting, these attacks have originated primarily from a single group of attackers known as Hafnium. The Exchange Server Team has released a script for checking Hafnium Indicators of Compromise (IOCs) on GitHub. System owners are encouraged to update on-premise systems and check against the provided IOCs. More information can be found at https://github.com/microsoft/CSS-Exchange/tree/main/Security & https://www.fireeye.com/blog/threat-research/2021/03/detection-response-to-exploitation-of-microsoft-exchange-zero-day-

RESEARCHER OF THE MONTH

We are excited to announce the February 2021 DoD VDP Researcher of the Month Award goes to Hemant "@HemantSolo" Patidar with HackerOne! Hemant submitted three critical and one high severity reports for variants of blind/stored #XSS that could lead to administrator access. The researcher also discovered twenty endpoint findings. Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program! Happy Hacking!

DC3 DOD CYBER CRIME CENTER