DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES JANUARY 2021

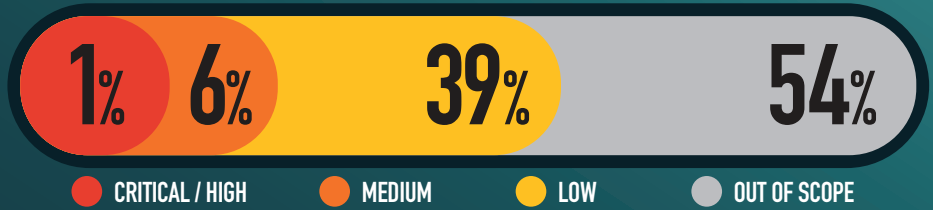## 26,617
VULNERABILITIES SINCE LAUNCH

2,283
RESEARCHERS SINCE LAUNCH

17,384
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

1%	6%	39%	54%
CRITICAL / HIGH	MEDIUM	LOW	OUT OF SCOPE

SUBMITTED VULNERABILITIES

JUL 2020	AUG 2020	SEP 2020	OCT 2020	NOV 2020	DEC 2020	JAN 2021
1,835	1,203	1,143	2,176	1,384	1,336	1,339

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE	547
CWE-840 BUSINESS LOGIC ERRORS	122
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	96
CWE-79 CROSS-SITE SCRIPTING	71
CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE	68

KNOWLEDGE BYTE

Since September 2020 our team has continued to receive vulnerabilities, detailed in CVE-2020-14179, by our researchers. This CVE addresses vulnerabilities in JIRA software that allow, if successfully exploited, attackers access to sensitive information by injecting arbitrary HTML or JavaScript via a Cross Site Scripting (XSS) vulnerability in the XML export view. All system owners, commercial and military, should address this issue by upgrading to the latest version of Atlassian JIRA Server. More information can be found at https://iavm.csd.disa.mil/iavm-notice-html/143049

RESEARCHER OF THE MONTH

We are excited to announce the January 2021 DoD VDP Researcher of the Month Award goes to Johnathan "nidens" Miranda with HackerOne! He submitted a critical IDOR vulnerability that if exploited could allow the intercept of thousands of medical records containing PHI/PII. Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program! Happy Hacking!

DC3
DOD CYBER CRIME CENTER