DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES APRIL 2022

40,401
VULNERABILITIES SINCE LAUNCH

3,331
RESEARCHERS SINCE LAUNCH

23,427
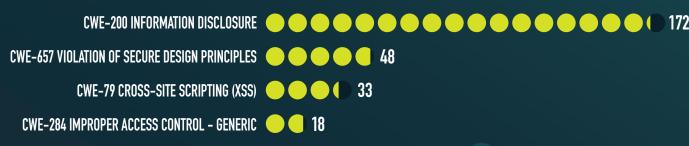ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

9% **11%** **21%** **59%**

● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

	OCT 2021	NOV 2021	DEC 2021	JAN 2022	FEB 2022	MAR 2022	APR 2022
	653	606	443	708	981	859	446

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE — 172

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 48

CWE-79 CROSS-SITE SCRIPTING (XSS) — 33

CWE-284 IMPROPER ACCESS CONTROL - GENERIC — 18

KNOWLEDGE BYTE

In April 2022, the DoD VDP received multiple critical reported findings affecting VMware Workspace ONE Access and Identity Manager (CVE-2022-22954). Improper input validation allowing a remote attacker to perform a server-side template injection through an HTTP request caused this vulnerability. VMware released a fix and workaround on April 6, which included fixes for seven other various flaws. System administrators should refer to VMware Security Advisories to determine affected applications and apply the appropriate VMware update. More information can be found at the following: https://iavm.csd.disa.mil/iavm-notice-html/144011 & https://www.vmware.com/security/advisories/VMSA-2002-0011.html

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for April 2022 is **adgn** with HackerOne. They submitted a critical severity report that allowed the unauthenticated alteration of the config file of a DoD network device with Cisco Smart Install Protocol! VDP Hackers for the win!