# BUG BYTES MARCH 2022

## 39,954
VULNERABILITIES SINCE LAUNCH
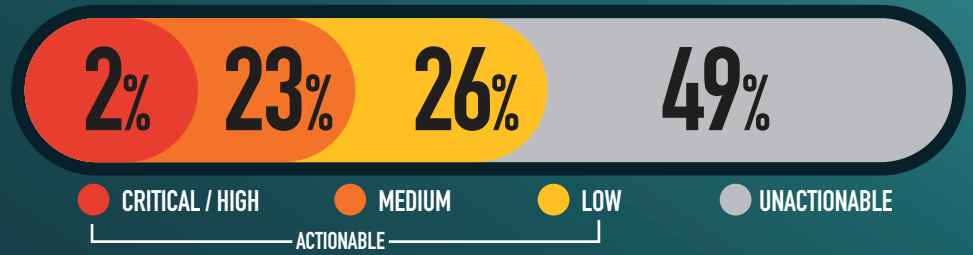
## 3,257
RESEARCHERS SINCE LAUNCH

## 23,064
ACTIONABLE REPORTS PROCESSED
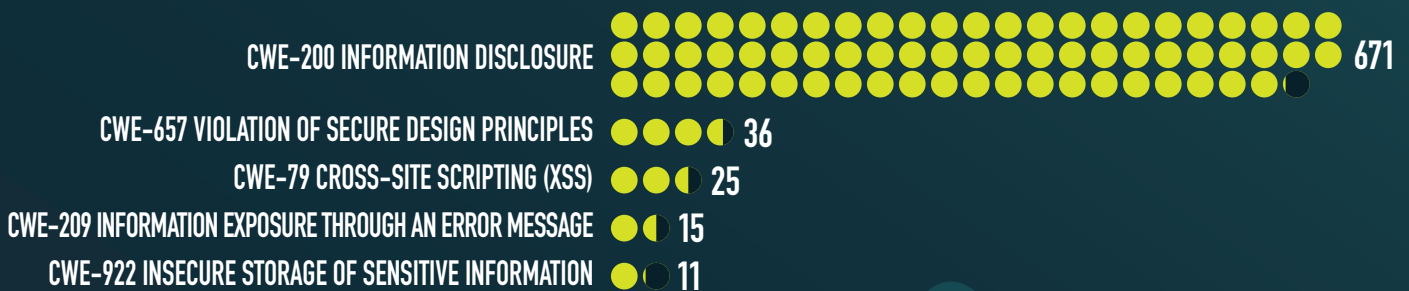
## SEVERITY FOR THE MONTH

| 2% | 23% | 26% | 49% |
|---|---|---|---|
| CRITICAL / HIGH | MEDIUM | LOW | UNACTIONABLE |

ACTIONABLE

## SUBMITTED VULNERABILITIES

| | SEP 2021 | OCT 2021 | OCT 2021 | DEC 2021 | JAN 2022 | FEB 2022 | MAR 2022 |
|---|---|---|---|---|---|---|---|
| | 799 | 653 | 606 | 443 | 708 | 981 | 859 |

## LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE — 671

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 36

CWE-79 CROSS-SITE SCRIPTING (XSS) — 25

CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE — 15

CWE-922 INSECURE STORAGE OF SENSITIVE INFORMATION — 11

## KNOWLEDGE BYTE

In March 2022, the DoD VDP received a critical reported finding for a pre-auth Remote Code Execution (RCE) vulnerability in ForgeRock Access Manager before version 7.0 (CVE-2021-35464). The exploitation does not require authentication, allowing an attacker to execute commands in the context of the current user to gain credentials and certificates. This is due to an unsafe Java deserialization in the Jato framework used by OpenAM. System owners should update to version 7.1.0 or later or refer to the ForgeRock Security Advisory to determine affected applications and appropriate fix actions. See the following for more information: https://iavm.csd.disa.mil/lavm-notice-html/143702 & https://portswigger.net/research/pre-auth-rce-in-forgerock-openam-cve-2021-35464

## RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for March 2022 is **@tyrantsec**. They submitted multiple high severity reports this month that showed PII being exposed that had not been properly redacted before being posted! VDP Hackers for the win!