DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES AUGUST 2025

57,062
VULNERABILITIES SINCE LAUNCH
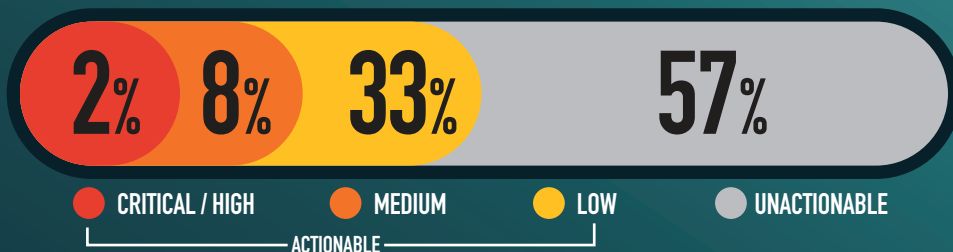
7,693
RESEARCHERS SINCE LAUNCH

30,927
ACTIONABLE REPORTS PROCESSED

139
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH

2% **8%** **33%** **57%**

● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

Month	Value
FEB 2025	391
MAR 2025	497
APR 2025	385
MAY 2025	297
JUN 2025	388
JUL 2025	414
AUG 2025	300

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-284 IMPROPER ACCESS CONTROL - GENERIC ●● **89**
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●●●●●●●●●●●●●●●●●●●●●●●●●● **42**
CWE-200 INFORMATION DISCLOSURE ●●●●●●●●●●●●●●●●●●●●●●●●● **39**
CWE-601: OPEN REDIRECT ●●●●●●●●●● **16**
CWE-79 CROSS-SITE SCRIPTING ●●●●● **8**

KNOWLEDGE BYTE

In August 2025, the DoD VDP received a high severity submission, CVE-2025-4123, identifying a path traversal vulnerability within Grafana that could lead to arbitrary code execution. Grafana is a dashboard used to compile, categorize, and query data sets. Researchers identified a weakness that allowed the Grafana server to be redirected to an attacker-controlled repository and execute JavaScript through custom-crafted plugins. It is recommended that all system owners update to the latest approved version of Grafana. Further information is available in the following resources: https://grafana.com/blog/2025/05/23/grafana-security-release-medium-and-high-severity-security-fixes-for-cve-2025-4123-and-cve-2025-3580/ & https://nvd.nist.gov/vuln/detail/CVE-2025-4123 & https://iavm.csd.disa.mil/iavm-notice-html/146835

RESEARCHER OF THE MONTH

Huge congratulations to **@sherifx_x** for being named *Researcher of the Month*. **@sherifx_x** is being recognized for finding an arbitrary file upload vulnerability and producing a full RCE payload within an Avaya Aura Device Services deployment. Well deserved! **#CyberSecurity #InfoSec #WebSecurity #PrivacyMatters**