DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES DECEMBER 2024

53,872
VULNERABILITIES SINCE LAUNCH
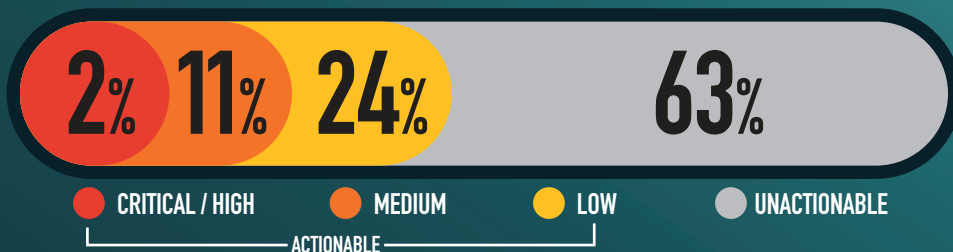
6,984
RESEARCHERS SINCE LAUNCH

29,560
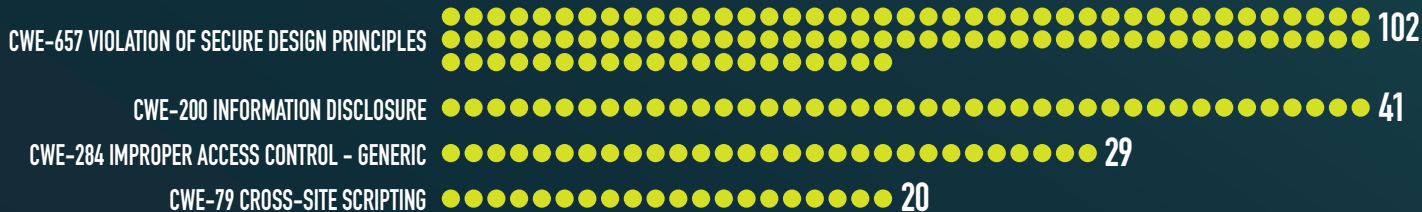ACTIONABLE REPORTS PROCESSED

115
ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH

2% **11%** **24%** **63%**

● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

Month	Value
JUN 2024	410
JUL 2024	957
AUG 2024	321
SEP 2024	333
OCT 2024	309
NOV 2024	183
DEC 2024	296

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 102

CWE-200 INFORMATION DISCLOSURE — 41

CWE-284 IMPROPER ACCESS CONTROL - GENERIC — 29

CWE-79 CROSS-SITE SCRIPTING — 20

KNOWLEDGE BYTE

In December 2024, The DoD VDP received a critical severity submission detailing a vulnerability that allowed for the extraction of database contents from a Lotus Domino server. Lotus Domino is a workflow application that uses notes and agents to assist in serving various web applications. Researchers discovered a weakness in a Domino user agent security permission. By specifying certain requests, sensitive database information can be read such as account names and password hashes. System owners are encouraged to review all interactive databases and confirm any sensitive information has restricted access. More information:
https://help.hcl-software.com/domino/10.0.1/admin/conf_restrictingaccesstoaserversdatadirectory_t.html
https://help.hcl-software.com/dom_designer/12.0.0/basic/h_setup_agent_security_steps.html
https://security.berkeley.edu/education-awareness/database-hardening-best-practices

RESEARCHER OF THE MONTH

Kudos to **Roy Solberg** (**@roysolberg**) for an outstanding end-of-year contribution! Identifying numerous exploits in one month including RXSS, SSRF, unauthorized account approvals, file uploads, and database extractions, your efforts have significantly bolstered DoD security. Thank you for your dedication! #CyberSecurity #InfoSec #DoDVDP