BUG BYTES DECEMBER 2023

49,318
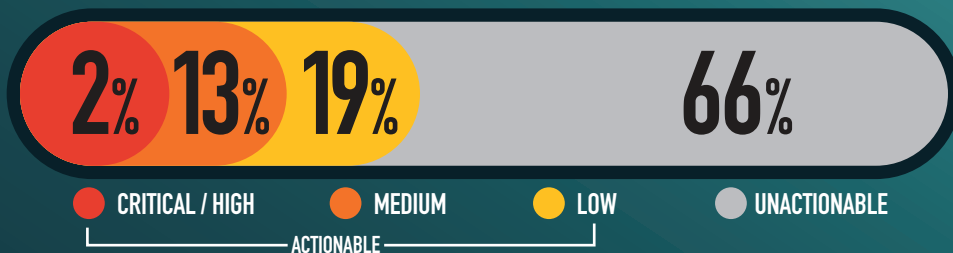VULNERABILITIES SINCE LAUNCH

5,527
RESEARCHERS SINCE LAUNCH

27,820
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

2% **13%** **19%** **66%**

● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

	JUN 2023	JUL 2023	AUG 2023	SEP 2023	OCT 2023	NOV 2023	DEC 2023
	201	711	240	267	542	262	284

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE — 84

CWE-284 IMPROPER ACCESS CONTROL - GENERIC — 40

CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE — 37

CWE-922 INSECURE STORAGE OF SENSITIVE INFORMATION — 29

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES — 17

KNOWLEDGE BYTE

In December 2023, the DoD VDP received a submission demonstrating unauthorized access to local system files through a vulnerability found in various Red Hat pki-core packages. Researchers utilized a technique known as XML External Entity Processing (XXE) to craft custom XML requests bypassing the server's parser. They used the requests to disclose critical operating system files containing configuration information along with information regarding local accounts stored on the server. It is recommended system owners review and update any affected system. See the following for more information: https://nvd.nist.gov/vuln/detail/CVE-2022-2414 & https://access.redhat.com/security/cve/cve-2022-2414 & https://owasp.org/www-community/vulnerabilities/XML_External_Entity_(XXE)_Processing

RESEARCHER OF THE MONTH

🎉 Celebrating the dawn of 2023 with cyber brilliance! ☀️ A thunderous applause for **Oxylis**, our Researcher of the Month! 🚀 His safeguarding prowess on a DoD asset shields us from potential data leaks. 🛡️ Let the New Year of cybersecurity triumphs begin! 💻✨ #ResearcherOfTheMonth #DODVDP #NewYearSecurity #CyberGuardian

Discover more: **https://hackerone.com/oxylis** 🌐🔒

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3
DOD CYBER CRIME CENTER