DOD VULNERABILITY DISCLOSURE PROGRAM
BUG BYTES OCTOBER 2023
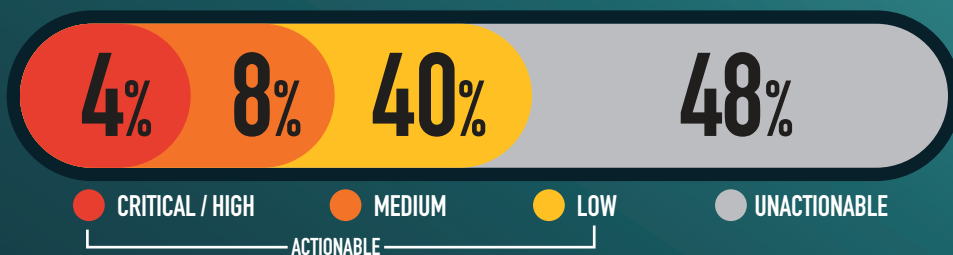
48,772
VULNERABILITIES SINCE LAUNCH

5,215
RESEARCHERS SINCE LAUNCH

27,602
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

4% **8%** **40%** **48%**

● CRITICAL / HIGH ● MEDIUM ● LOW ● UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES

APR 2023	MAY 2023	JUN 2023	JUL 2023	AUG 2023	SEP 2023	OCT 2023
323	225	201	711	240	267	542

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●●●●●●●●●●●●●● 138

CWE-200 INFORMATION DISCLOSURE ●●●●●●●●●●●● 105

CWE-284 IMPROPER ACCESS CONTROL - GENERIC ●●●● 32

CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE ●● 20

KNOWLEDGE BYTE

In October 2023, the DoD VDP received multiple submissions demonstrating a condition where unauthorized users could retrieve active session tokens used by Citrix NetScaler. Citrix NetScaler is software used for remote application access and delivery. By creating custom HTTP requests, researchers were able to overflow the memory buffer and access session token information. It is recommended system owners utilizing Citrix NetScaler deploy the latest updated versions. See the following for more information: https://support.citrix.com/article/CTX579459/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20234966-and-cve20234967 & https://nvd.nist.gov/vuln/detail/CVE-2023-4966 & https://services.google.com/fh/files/misc/citrix-netscaler-adc-gateway-cve-2023-4966-remediation.pdf

RESEARCHER OF THE MONTH

🎃🕷 Our spooktacular DOD Vulnerability Disclosure Program Researcher of the Month for October is none other than **@reginaldojsf!** They've exorcised a wicked remote code execution bug from the Royal Elementor Addons plugin. We're bewitched by their skills! 🌟👻 #Cybersecurity #ResearcheroftheMonth! VDP Hackers for the win!