DOD VULNERABILITY DISCLOSURE PROGRAM

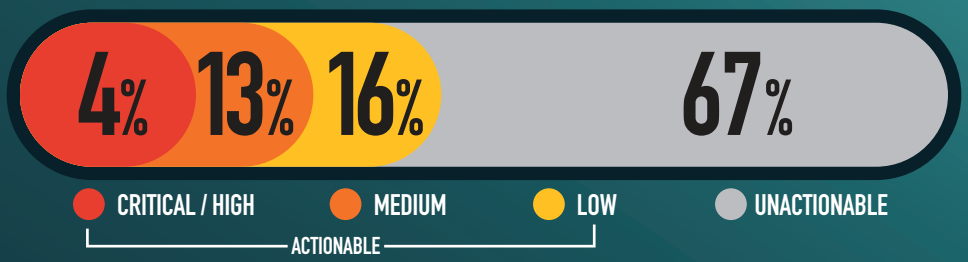
BUG BYTES JANUARY 2024

49,640
VULNERABILITIES SINCE LAUNCH

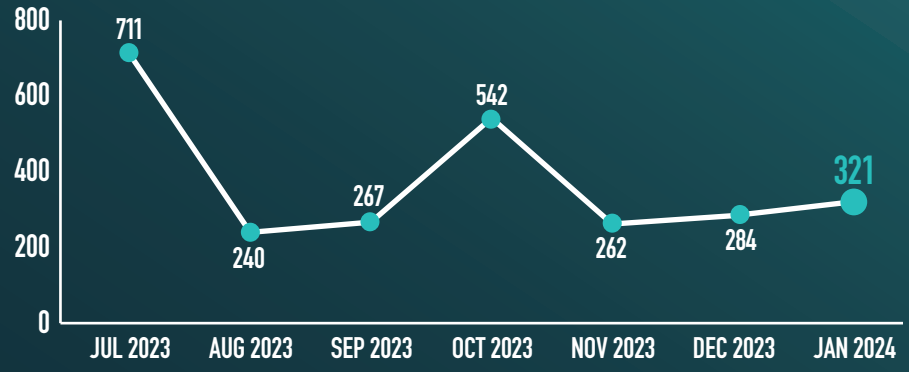
5,635
RESEARCHERS SINCE LAUNCH

27,938
ACTIONABLE REPORTS PROCESSED

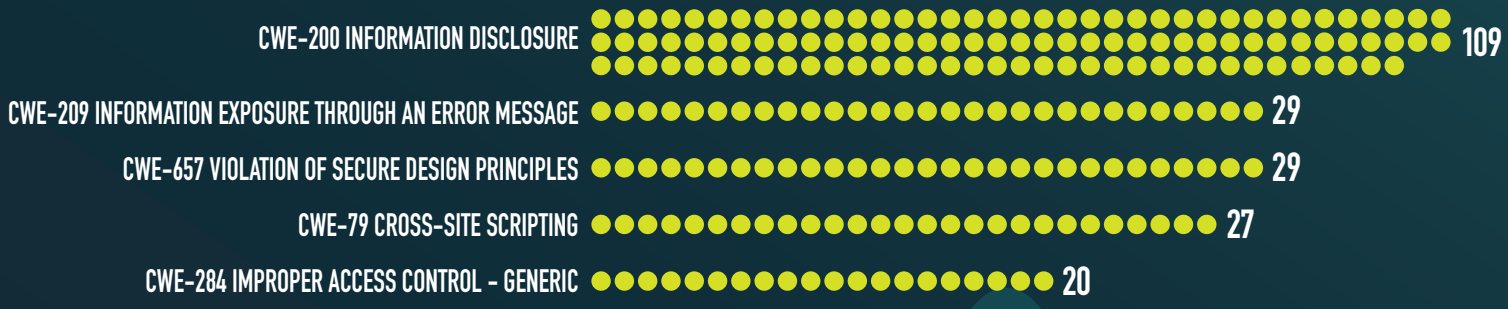
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH



KNOWLEDGE BYTE

In January 2024, a critical submission was received by the DoD VDP, showcasing CVE-2023-46747, an unauthenticated remote code execution (RCE) within unpatched F5 BIG-IP virtual appliances. Researchers identified vulnerabilities in older versions of these appliances regarding how they processed HTTP requests, enabling them to circumvent existing authentication controls. These requests demonstrated the potential of privilege escalation and unapproved access to restricted functions of the device. System owners are advised to review and update any affected appliances. Further information can be found in the following resources: https://nvd.nist.gov/vuln/detail/CVE-2023-46747 & https://my.f5.com/manage/s/article/K000137353 & https://www.praetorian.com/blog/refresh-compromising-f5-big-ip-with-request-smuggling-cve-2023-46747

RESEARCHER OF THE MONTH

🔴 Marching into 2024 with a cyber sentinel! 🏆 Salute to our January Researcher of the Month, @eleven_OO1. 🚀 Unearthed a DOD VDP treasure—a crucial vulnerability exposing credentials & IPs. Secure skies ahead! 💻🛡️ #DODvdp #CyberGuardian #ResearcherOfTheMonth #NewYearSecurity

𝕏 @DC3VDP
DC3.VDPQuestions@us.af.mil

DC3 DOD CYBER CRIME CENTER