

BUG BYTES JULY 2025



56,762

VULNERABILITIES SINCE LAUNCH

7,613

RESEARCHERS SINCE LAUNCH

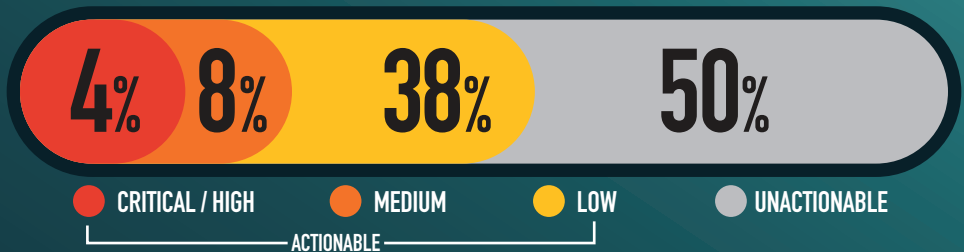
30,791

ACTIONABLE REPORTS PROCESSED

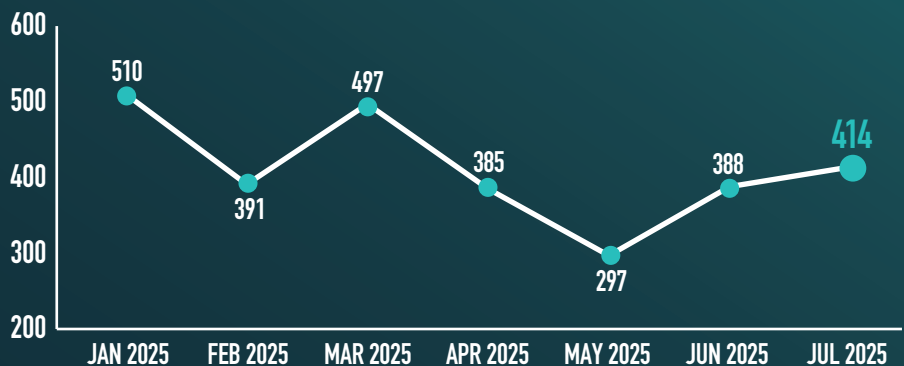
211

ACTIONABLE VDPS FOR THE MONTH

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	113
CWE-200 INFORMATION DISCLOSURE	39
CWE-79 CROSS-SITE SCRIPTING	38
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	31
CWE-119: MEMORY CORRUPTION - GENERIC	19

KNOWLEDGE BYTE

In July 2025, the DoD VDP received multiple critical severity submissions identifying CVE-2025-5777, a memory overread vulnerability found in specific configurations of Citrix NetScaler appliances. Citrix NetScaler is a multifaceted product designed for application delivery and remote access. Researchers were able to access a parameter that, when left empty, enabled access to the internal memory of the appliance. It is recommended that all system owners utilizing Citrix NetScaler update to the latest applicable version. Further information can be found in the following resources:

<https://support.citrix.com/external/article/693420/netscaler-adc-and-netscaler-gateway-secu.html> & <https://nvd.nist.gov/vuln/detail/CVE-2025-5777> & <https://docs.netscaler.com/en-us/netscaler-console-service/instance-advisory/remediate-vulnerabilities-cve-2025-5777.html>

RESEARCHER OF THE MONTH

👏 Congratulations to @0x2458 for being named *Researcher of the Month* by the DoD Vulnerability Disclosure Program! Your contributions are making a real impact on national cybersecurity. 🇺🇸 #DoD #VDP #CyberSecurity #BugBounty