

BUG BYTES OCTOBER 2025



57,820

VULNERABILITIES SINCE LAUNCH

7,764

RESEARCHERS SINCE LAUNCH

31,327

ACTIONABLE REPORTS PROCESSED

226

ACTIONABLE VDPs FOR THE MONTH

SEVERITY FOR THE MONTH

23%

8%

23%

46%



CRITICAL / HIGH



MEDIUM



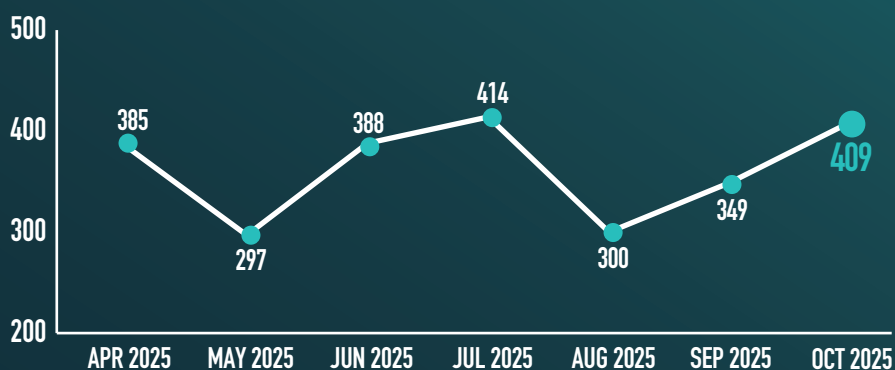
LOW



UNACTIONABLE

ACTIONABLE

SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	112
CWE-200 INFORMATION DISCLOSURE	71
CWE-122 HEAP OVERFLOW	67
CWE-120 BUFFER OVERFLOW	32
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	19

KNOWLEDGE BYTE

In October 2025, the DoD VDP received multiple critical severity submissions identifying a heap overflow attack within Cisco ASA devices that could result in remote code execution, as documented in CVE-2025-20333. Cisco ASA devices serve to provide networks with firewall, intrusion prevention, and VPN services. Researchers identified a weakness in the WebVPN feature that allowed additional command execution within memory. It is recommended that all system owners install the latest approved ASA software. Further information is available in the following resources: <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asafld-webvpn-z5xP8EUB> & <https://www.cisa.gov/news-events/directives/ed-25-03-identify-and-mitigate-potential-compromise-cisco-devices> & <https://www.rapid7.com/blog/post/etr-cve-2025-20333-cve-2025-20362-cve-2025-20363-multiple-critical-vulnerabilities-affecting-cisco-products/>

RESEARCHER OF THE MONTH

Huge congratulations to @yaser_s for being named Researcher of the Month. @yaser_s is being recognized for finding an authentication bypass and buffer overflow vulnerability on Cisco ASA, which could have led to RCE on affected devices. 🏆 Well deserved!
#CyberSecurity #VDP