DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE OCTOBER 2025

DIB-VDP

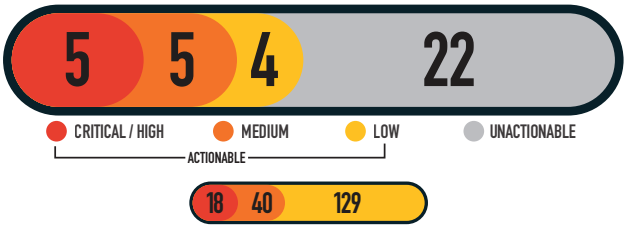
948
VULNERABILITIES SUBMITTED SINCE LAUNCH

36
VULNERABILITIES FOR THE MONTH

256
RESEARCHERS SINCE LAUNCH

14
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

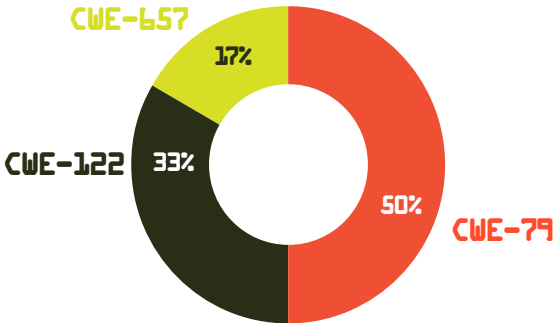


MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH

- 2 Successful Mitigations (Including Top 5 Organization Data)
- 0 Unsuccessful Attempts

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-79 CROSS-SITE SCRIPTING XSS: 6
CWE-122 HEAP OVERFLOW: 4
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 2

KNOWLEDGE BYTE

In October 2025, the DIB-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-asaftd-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

Big thanks to @alfred05 for reporting a **Reflected XSS** vulnerability through our **#DIBVDP** program! 🎯 This type of flaw can allow attackers to inject malicious scripts, steal session data, or perform unauthorized actions on behalf of users. **#CyberSecurity #InfoSec #WebSecurity #EthicalHacking**

TOP VULNERABILITIES SINCE LAUNCH