DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM

MYTE BYTE MARCH 2026

DIB-VDP

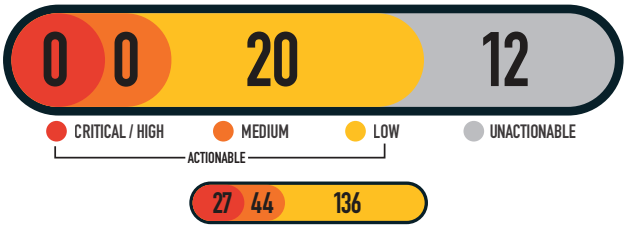
1044
VULNERABILITIES SUBMITTED SINCE LAUNCH

32
VULNERABILITIES FOR THE MONTH

289
RESEARCHERS SINCE LAUNCH

20
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

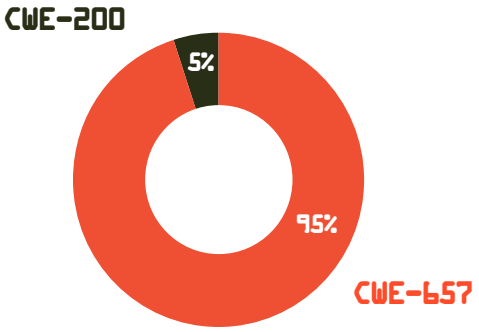


MITIGATED VULNERABILITIES BY SEVERITY SINCE LAUNCH

MITIGATIONS FOR THE MONTH

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

VULNERABILITY TYPES/ LEADING CWE'S FOR THE MONTH



CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES: 19
CWE-200 INFORMATION DISCLOSURE: 1

KNOWLEDGE BYTE

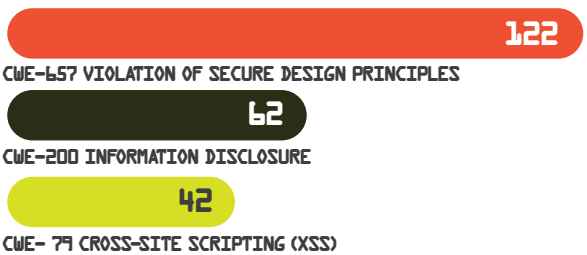
In March 2026, a critical vulnerability was identified impacting the defense industrial base: CVE-2026-20127, an authentication bypass flaw in Cisco Catalyst SD-WAN Controller and Manager. Cisco SD-WAN is widely deployed across the DIB to connect contractor sites, data centers, and military installations carrying CUI and ITAR-scoped data. Security researchers and intelligence partners identified that a sophisticated nation-state threat cluster (UAT-8616) had been exploiting this vulnerability as a zero-day since 2023, enabling unauthenticated attackers to gain privileged access, insert rogue devices into SD-WAN fabrics, and erase forensic evidence. CISA responded with Emergency Directive ED 26-03 and a joint NSA/Five Eyes advisory from six nations. Organizations utilizing Cisco SD-WAN are strongly encouraged to apply the latest approved updates and conduct threat hunting per CISA supplemental guidance to mitigate this risk. Further technical details and guidance are available in the following resources:

https://www.cisa.gov/news-events/directives/ed-26-03
https://www.intel471.com/blog/cve-2026-20127
https://www.defendedge.com/cisa-and-partners-release-guidance-ongoing-global-exploitation-cisco-sd-wan-systems/

RESEARCHER OF THE MONTH

Big thanks to @mdjab3r for identifying a missing DMARC record. Without DMARC, domains are far more vulnerable to email spoofing, phishing, and brand impersonation—putting users and organizations at serious risk. **#DIBVDP #CyberSecurity #InfoSec #WebSecurity #EthicalHacking**

TOP VULNERABILITIES SINCE LAUNCH



@DC3VDP
AFOSI.DC3.DIB-VDP@us.af.mil

DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY