DOD DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM PILOT

MYTE BYTE

OCTOBER 2021

DIB-VDP

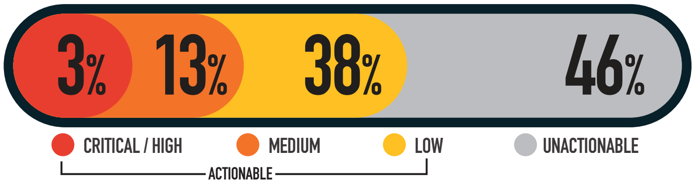
887 VULNERABILITIES SINCE LAUNCH

37 VULNERABILITIES FOR THE MONTH

230 RESEARCHERS SINCE LAUNCH

29 ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH

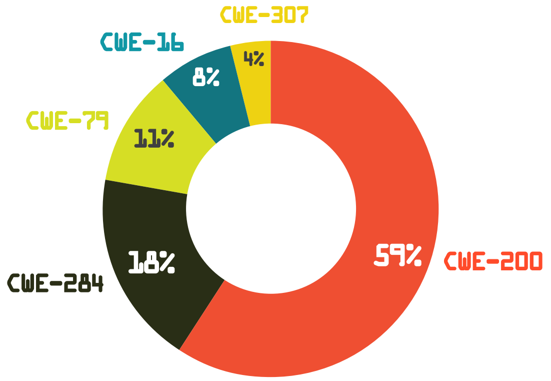


MITIGATIONS FOR THE MONTH

● 3 Successful Mitigations (Including Top 5 Organization Data)

● 0 Unsuccessful Attempts

VULNERABILITY TYPES/LEADING CWE'S FOR THE MONTH



CWE-200 INFORMATION DISCLOSURE: 16

CWE-284 IMPROPER ACCESS CONTROL- GENERIC: 5

CWE-79 CROSS-SITE SCRIPTING (XSS): 3

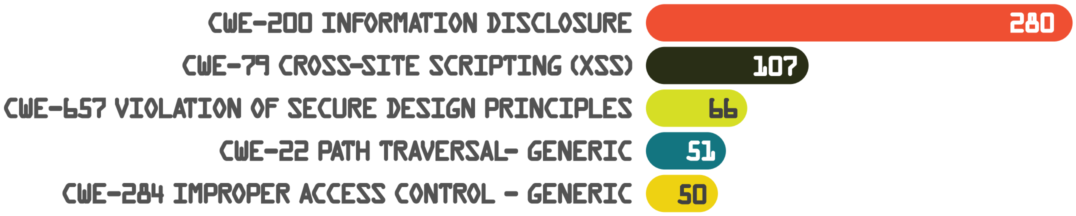
CWE-16 MISCONFIGURATION: 2

CWE-307 BRUTE FORCE: 1

KNOWLEDGE BYTE

The DIB-VDP received notification of an asset vulnerable to CVE-2021-26084, a critical severity exploitable vulnerability in a public-facing asset. An OGNL injection vulnerability exists that would allow an unauthenticated user to execute arbitrary code on a Confluence Server or Data Center instance. Application versions before version 6.13.23, from version 6.14.0 before 7.4.11, from version 7.5.0 before 7.11.6, and from version 7.12.0 before 7.12.5 are affected by this vulnerability. The vulnerability is exploitable by unauthenticated users regardless of configuration. The vendor reports it is being actively exploited in the wild. Affected servers should be patched immediately. If you are unable to upgrade Confluence immediately, then as a temporary workaround, you can mitigate the issue by running the script provided by the vendor for the Operating System that Confluence is hosted on: https://nvd.nist.gov/vuln/detail/CVE-2021-26084

TOP VULNERABILITIES SINCE LAUNCH



@DC3VDP
DIB-VDP@DC3.mil

DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY