



40,760

VULNERABILITIES SINCE LAUNCH

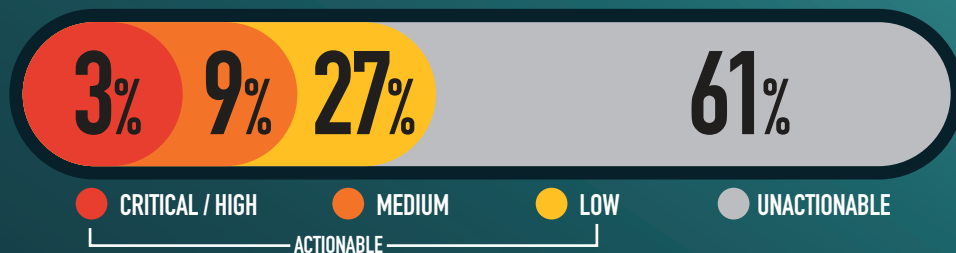
3,395

RESEARCHERS SINCE LAUNCH

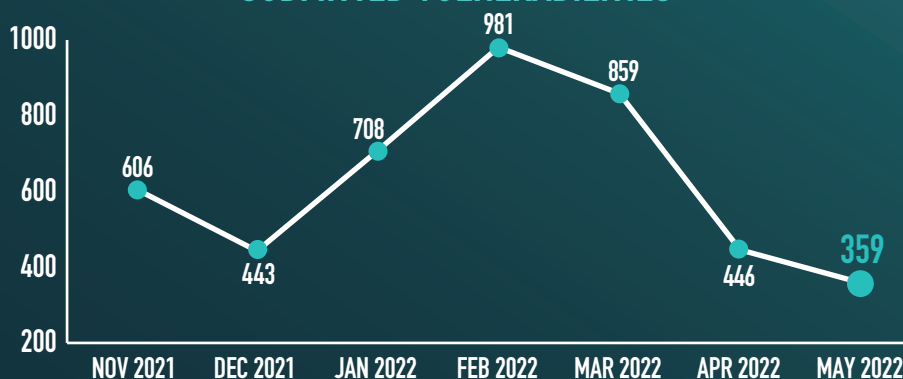
23,563

ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE ●●●●●●●●●●●●●●●● 115

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●●●●●●●● 56

CWE-548 INFORMATION EXPOSURE THROUGH DIRECTORY LISTING ●●●●●●●● 31

CWE-284 IMPROPER ACCESS CONTROL - GENERIC ●●●●●●●● 23

KNOWLEDGE BYTE

Atlassian has released a security advisory regarding a vulnerability (CVE-2022-26134) in Confluence Server, which, if exploited, could allow an unauthenticated user to execute arbitrary code on the system. This vulnerability uses command injections using specially crafted strings to load a malicious file in memory, allowing attackers to plant a web shell on the machine. JFHQ-DODIN is unaware of any DoD-related incidents; however, system administrators should refer to the Atlassian Security Advisories to determine affected applications and appropriate fix actions.

More information can be found at the following:

<https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html>

<https://iavm.csd.disa.mil/iavm-notice-html/144130>

<https://blog.cloudflare.com/cloudflare-observations-of-confluence-zero-day-cve-2022-26134/>

RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for May 2022 is @100801. They submitted a critical severity report that showed default admin credentials were still configured on an application running on a DoD server! VDP Hackers for the win!