

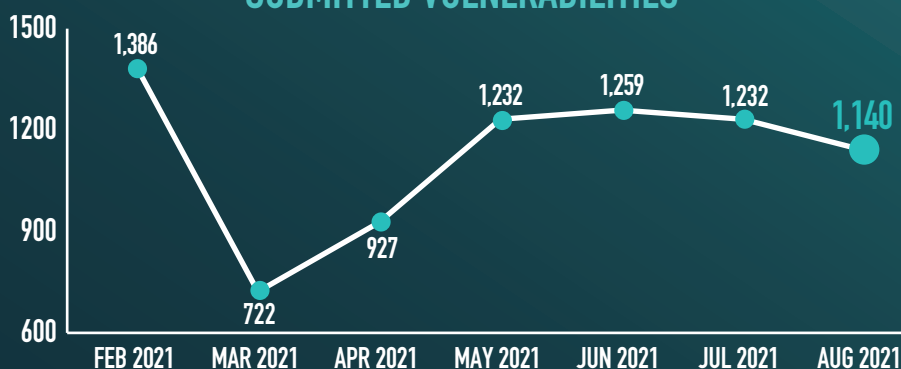
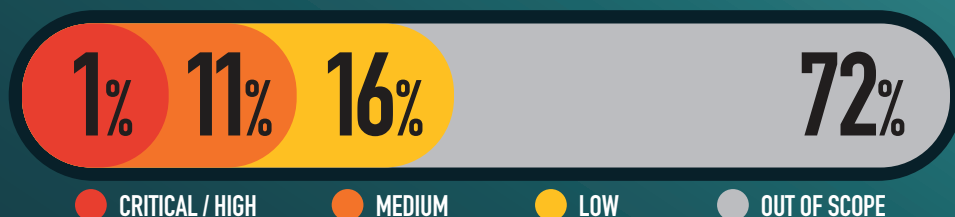


34,577

2,894

17,920

ACTIONABLE REPORTS PROCESSED



CWE-200 INFORMATION DISCLOSURE 404

CWE-79 CROSS-SITE SCRIPTING (XSS) ●●●●●●●●●●●●●●●● 333

CWE-922 INSECURE STORAGE OF SENSITIVE INFORMATION ●●●●● 99

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLE ●●● 57

CWE-601 OPEN REDIRECT ●● 37

Approaching the end of August, the DoD VDP received multiple, critical RCE submissions affecting Atlassian Confluence Server (CVE-2021-26084). An OGNL injection vulnerability exists that would allow an authenticated user, and in some instances an unauthenticated user, to execute arbitrary code on a Confluence Server or Data Center instance. System owners are encouraged to refer to the Atlassian Security Advisory to determine the appropriate fix actions. At this time, JFHQ-DODIN is not aware of any DoD related instances. More information can be found at the following: <https://iavm.csd.disa.mil/iavm-notice-html/143757/> <https://jira.atlassian.com/browse/CONFSERVER-67940>

We are excited to announce the August 2021 DoD VDP Researcher of the Month Award goes to [@willyc0de](#). They submitted a high severity report this month where they showed a misconfigured DoD server that still allowed logins with default credentials! Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program! Happy Hacking!