DoD CYBER CRIME CENTER AND
DEFENSE COUNTERINTELLIGENCE
& SECURITY AGENCY

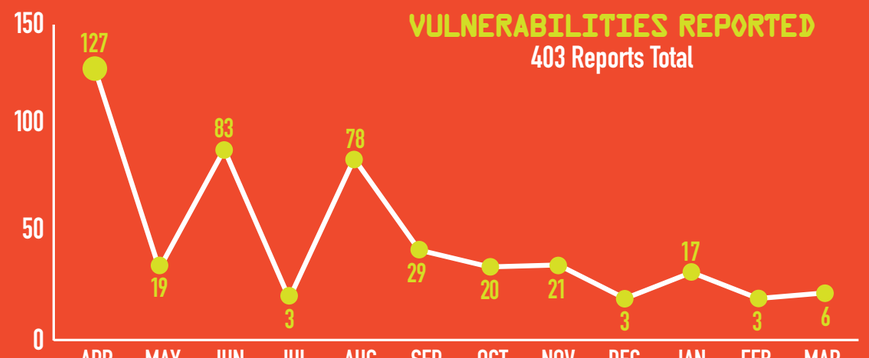
DIB-VDP PILOT

FINAL REPORT

TRENDING REPORTS

On October 30th, 2021, DIB-VDP Pilot received a ticket submission for CVE-2021-26084 affecting one of our DIB participant's confluence servers or Data Center instances. An Object-Graph Navigation Language (OGNL) injection vulnerability exists that would allow an unauthenticated attacker to execute arbitrary code on a Confluence Server or Data Center instance. This CVE affects versions older than 6.13.21, between 6.14.0 and 7.4.11, between 7.5.0 and 7.11.5, and between 7.12.0 and 7.12.5. The researcher was able to use this CVE to force our DIB participant's confluence server to execute any command or code on the target device.

https://nvd.nist.gov/vuln/detail/CVE-2021-26084

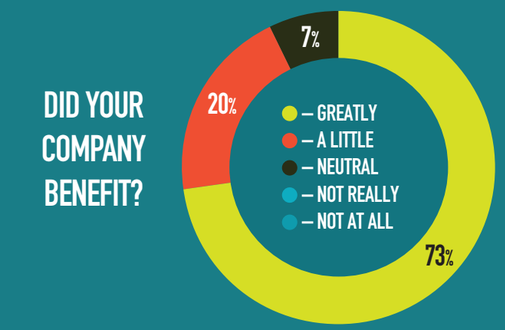


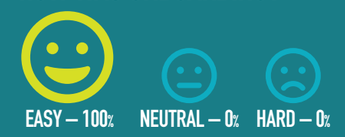
DIB-VDP Pilot received notifications, on April 29th, 2021, that two of our DIB participant's systems were vulnerable to CVE-2020-3187. A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. The researcher was able to send a crafted HTTP request containing directory traversal character sequences due to the lack of proper input validation of the HTTP URL. This could allow an unauthenticated, remote attacker to conduct directory traversal attacks and obtain read and delete access to sensitive files on a targeted system. These types of files exposed include: WebVPN configuration, Bookmarks, Web Cookies, Partial web content, HTTP URLs. If you don't want anyone stealing your favorite cookies, simply update to the latest version of Cisco.

https://nvd.nist.gov/vuln/detail/CVE-2020-3187

DIB-VDP PILOT PROGRAM SURVEY

The results are in...

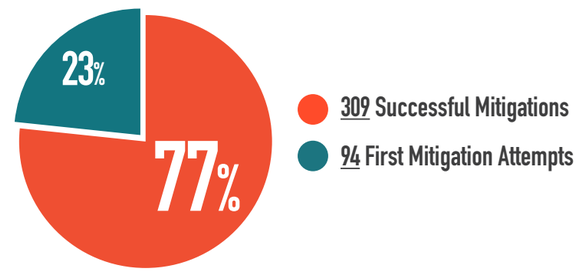




55½
AVERAGE DURATION IN DAYS OF MITIGATION BY PARTICIPANT

288
RESEARCHERS SINCE LAUNCH

41
PARTICIPANT COMPANIES



DIB-VDP TIMELINE

APR 2021
1st Mini Summit - **228** attended
DIB-VDP Pilot launched
Onboarded **14** new participants
141 initial assets added

MAY 2021
It was decided that we would continue onboarding every **60 days** due to overwhelming requests to join after the initial launch

JUN 2021
2nd Mini Summit - **41** attended
Onboarded **13** new participants
31 additional assets added

AUG 2021
3rd Mini Summit - **155** attended
Onboarded **5** new participants
102 additional assets added

OCT 2021
4th Mini Summit - **188** attended
Onboarded **6** new participants
17 additional assets added

JAN 2022
5th Mini Summit - **252** attended
Onboarded **2** new participants
56 additional assets added

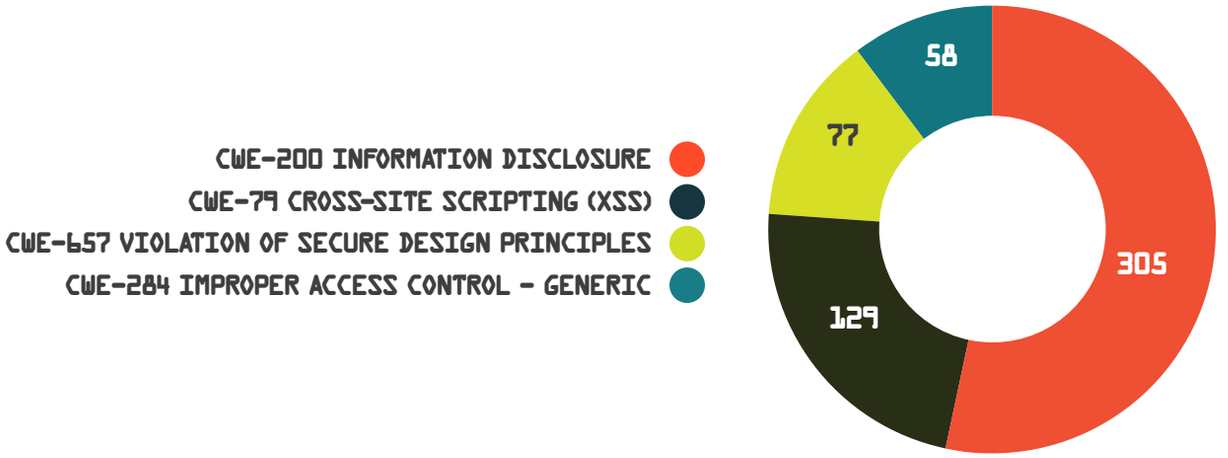
MAR 2022
Hot Wash held with DIBCO participants to answer questions regarding DIB-VDP Pilot closeout

APR 2022
DIBCO assets removed from **HackerOne**
No new reports accepted
Open report remediation concluded

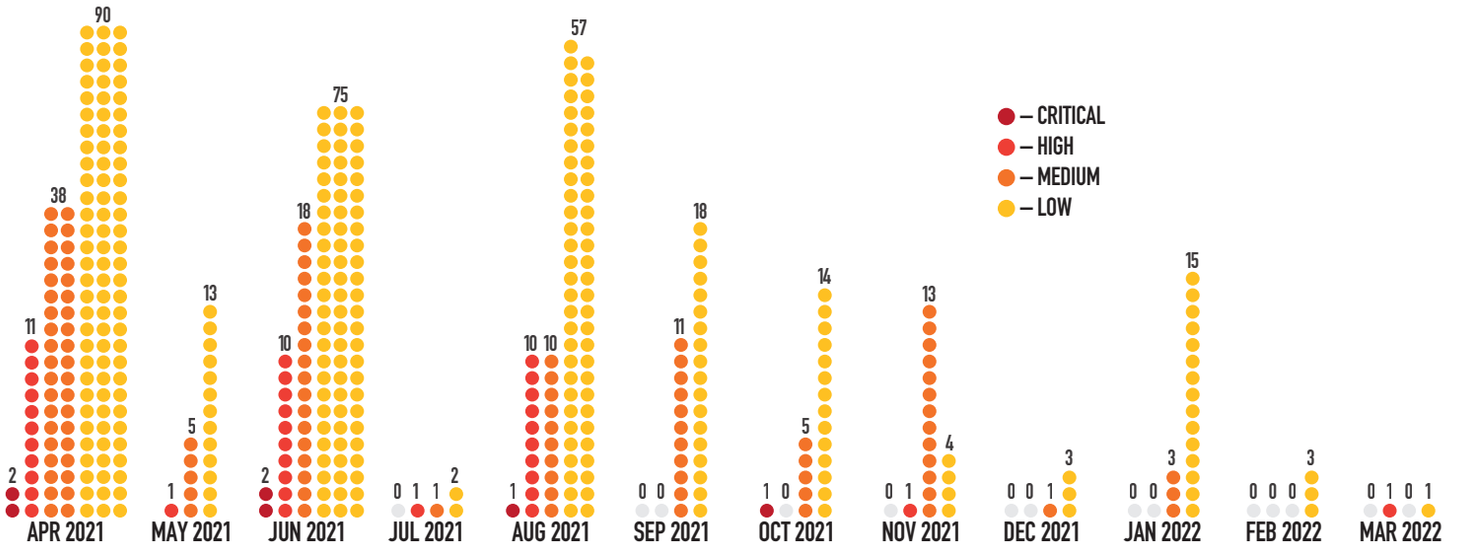
JUL 2022
DIB VRMN shut down

AUG 2022
Participant's **Slack** channels removed

TOP VULNERABILITIES REPORTED SINCE LAUNCH



VULNERABILITIES REPORTED BY MONTH



MOST IMPACTFUL REPORTS SINCE LAUNCH