DoD CYBER CRIME CENTER AND
DEFENSE COUNTERINTELLIGENCE
& SECURITY AGENCY

DIB-VDP PILOT

2021 ANNUAL REPORT

EXECUTIVE DIRECTOR MESSAGE

2021 was a year of distinctive successes for the Defense Industrial Base (DIB) Vulnerability Disclosure Program (VDP). This year DC3 had the pleasure of providing planning, execution, and oversight for the dual partnered DIB-VDP Pilot.

The DIB-VDP Pilot Annual Report highlights the efforts of the DIB-VDP Pilot and its stakeholders, respectively. 2021 is a time to reflect on the white hat researchers' positive impact on the DIB-VDP Pilot. VDP's passion remained consistent through the peaks and valleys of CoVID-19. With the help of the crowd-sourced researcher community, the DoD VDP team reached two significant milestones.

The first milestone of 2021 was the initial launch of the DIB-VDP Pilot on 5 April 2021, following the issuing of the DoD VDP Scope Expansion, which increased the range from only DoD websites to all DoD publicly accessible information systems in January 2021.

The second milestone was the launch of the Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP) Pilot. The jointly executed DC3 and Defense Counterintelligence and Security Agency DIB-VDP Pilot brings the five years of DoD VDP lessons learned to the pilot.

The expansion of in-scope assets for the DIB-VDP Pilot yielded an average of 50 to 80 reports per month to total 1019 reports for 2021. The ethical hacking community remained vigilant and dedicated to vulnerability discovery by submitting 441 new findings on the 248 DIB-VDP Pilot assets.

White hat researcher continuous engagement and feedback enhance the DIB-VDP Pilot by promoting DoDIN cyber hygiene and yields opportunities for recognition and increased reputation. The detail-oriented technical submissions of the former Researchers of the Month and Researchers of the Year resulted in 44 critical/high severity findings. They included unpatched Cisco devices susceptible to CVE-2020-3187 & CVE-2020-3452 and GitHub portals with exploitable remote code execution, file deletion, defamation, or content injection weaknesses.

The team is postured for readiness and the acceleration of change during 2022. This could not be achieved without the VDP researchers' commitment that bolsters the defenses of the DoD's public-facing cyber infrastructure.

V/r,

Jeffery D. Specht, SES, DAF
Executive Director (2018–2022)
DoD Cyber Crime Center (DC3)

"As a small business, it is often hard to allocate enough resources, or build out a proper security team, to face the ever growing cyber threat. Participation in the DIB-VDP program provided us an ability to supplement our team with security experts, which otherwise would have been too expensive to implement."

–DIB Participant Company

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

PARTICIPANT MESSAGE

The Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP) Pilot is a 12 month voluntary event established collaboratively by DC3's DoD Defense Industrial Base Collaborative Information Sharing Environment (DCISE), DoD Vulnerability Disclosure Program (DoD VDP), and the Defense Counterintelligence and Security Agency (DCSA).

We want to send a special thanks to all those that participated in the DIB-VDP Pilot and provide some additional feedback for best practices that might be useful in the future to further help all system owners. The most important thing is keeping your system up to date. This means installing patches released by the software developers created to fix known vulnerabilities which can be utilized to steal data, corrupt files, destroy infrastructures, and gain full access; access that could be undistinguishable to the untrained eye.

Keeping your systems on a regular patching schedule will not only limit the possibility of your systems, clients, and data being exposed to known vulnerabilities but also help insure that your applications and hardware are kept up to date.

Ensuring that your system is being regularly updated will also minimize the potential of data loss and application rewrites. The reason for this, and what is most often seen, is that the system owner has skipped numerous patches over a given time resulting in an overhaul of hardware and applications housed on the system. This overhaul often results in the system being taken down for an extended period.

The DIB-VDP Pilot Team celebrates our 12 month partnership, and we hope that you have a wonderful 2022 and look forward to future collaborative opportunities.

55½

AVERAGE DURATION IN DAYS OF MITIGATION BY PARTICIPANT

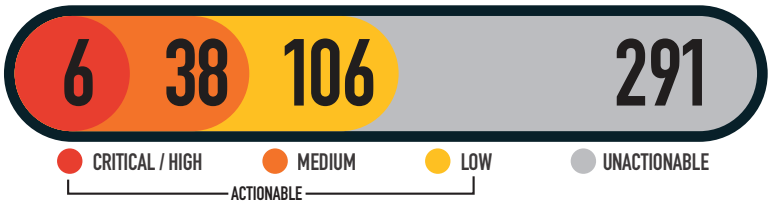
288

RESEARCHERS SINCE LAUNCH

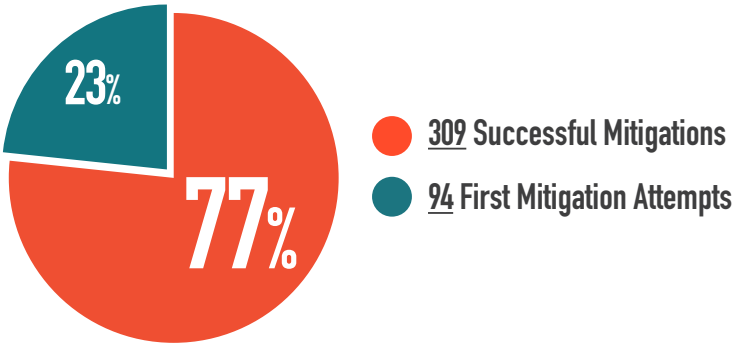
41

PARTICIPANT COMPANIES

VDPS BY SEVERITY SINCE LAUNCH



SINCE LAUNCH



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

2021 DIB-VDP RESEARCHER OF THE YEAR

Siavash Vaezafshar better known online as **@siavashvafshar** started reporting to the DIB-VDP Pilot in April 2021 with reports that were either not accepted due to scope or were duplicates of a reports already received. Over time and through perseverance he quickly started turning in high quality, technically savvy reports. Siavash went on a hot streak of highs and critical severity vulnerabilities in August, submitting 9 reports on various vulnerabilities ranging from Low to Critical findings

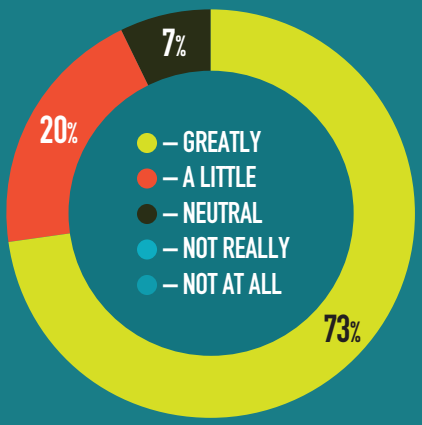
Siavash worked with the DIB-VDP Pilot staff through questions and maintained an open line of communication through the resolution process. He previously participated in our DOD VDP, as well as other VDP's and has been awarded monetarily for his efforts on other non-affiliated programs over the past 2 years. The DIB-VDP Pilot is happy to have Siavash as the 2021 Researcher of the Year. Through determination, dedication, communication and the willingness to work though challenges the vulnerabilities reported and resolved have saved the DIB-VDP Pilot and its participants time, money and effort in addition to significantly lowering their risk. Our team looks forward to what he can find in the upcoming years and wishes him and all our researchers good luck and happy hunting!

"The hardest hurdle to overcome was the initial implementation of the program. The initial influx of agents and their tools put a very strong load on our systems, and helped us identify configuration issues. Once those internal issues were resolved, the program progressed. Learning new tools, such as burp suite, while analyzing the cause of the discoveries has been very educational."

–DIB Participant Company

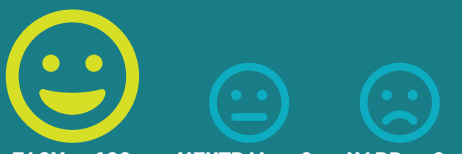
DIB-VDP PILOT PROGRAM SURVEY

The results are in...



DID YOUR COMPANY BENEFIT?

HOW WAS ONBOARDING?

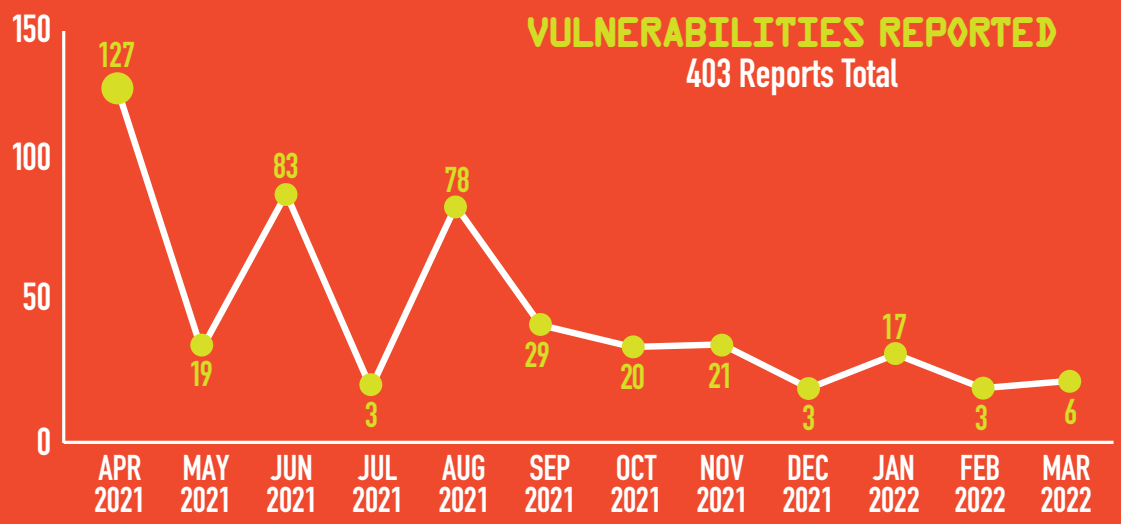


SHOULD THE PILOT CONTINUE?

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



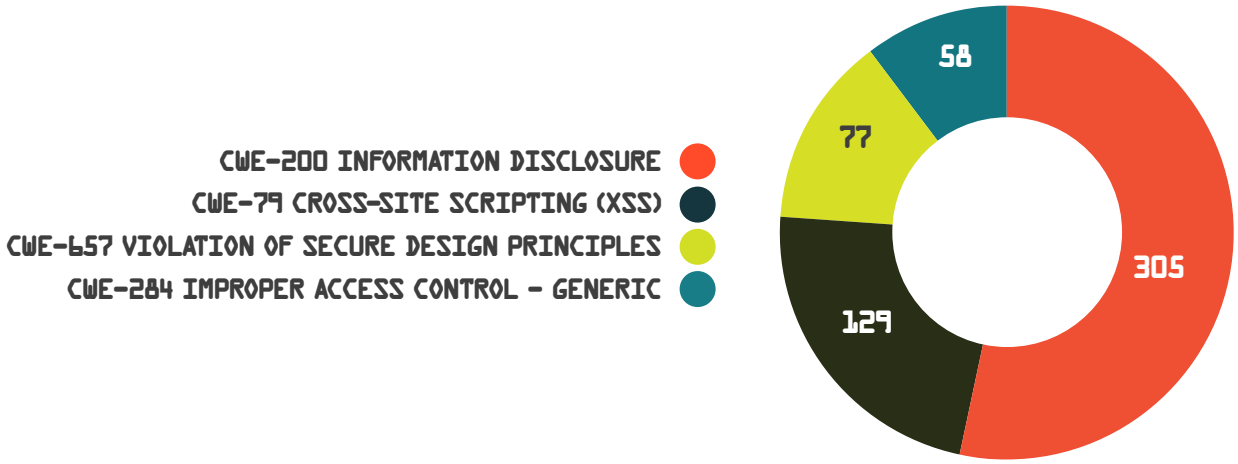
DIB-VDP Pilot received notifications, on April 29th, 2021, that two of our DIB participant's systems were vulnerable to CVE-2020-3187. A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. The researcher was 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

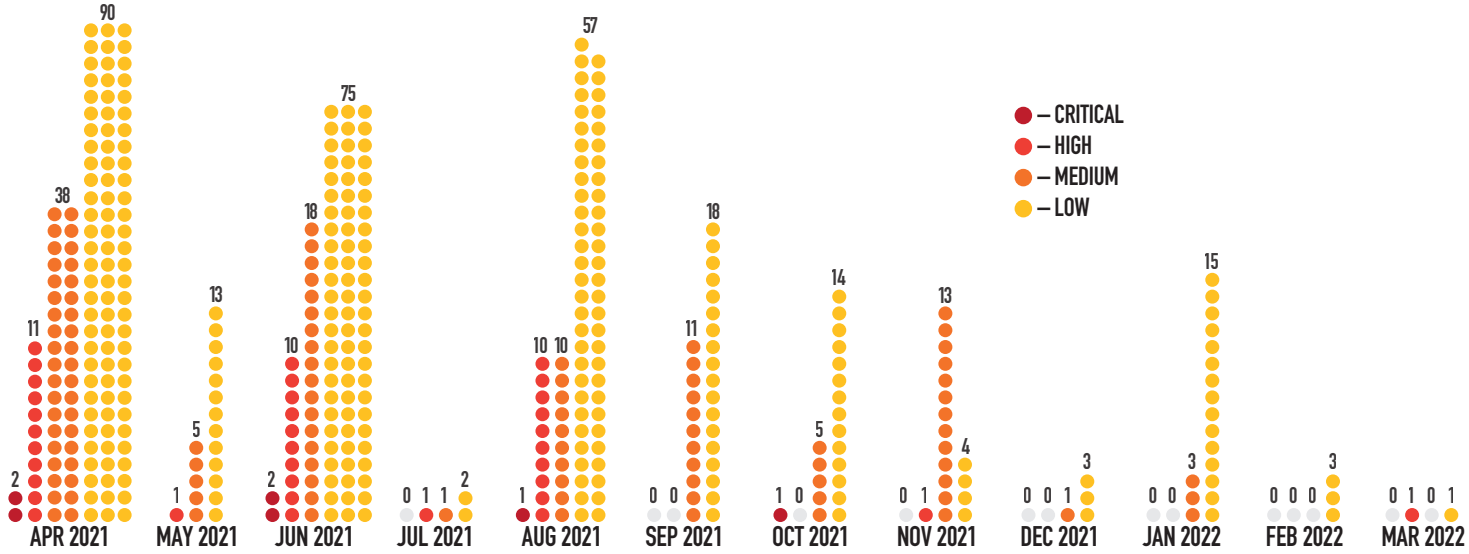
"One valuable aspect of the program, is seeing the process that other entities follow with their programs. The workflow of bug identification, validations, tasking, resolution and fix verification via the JIRA application has been extremely helpful. Also, the availability of the support teams via Slack has been much appreciated. Thank you for letting us be a part of the program."

–DIB Participant Company

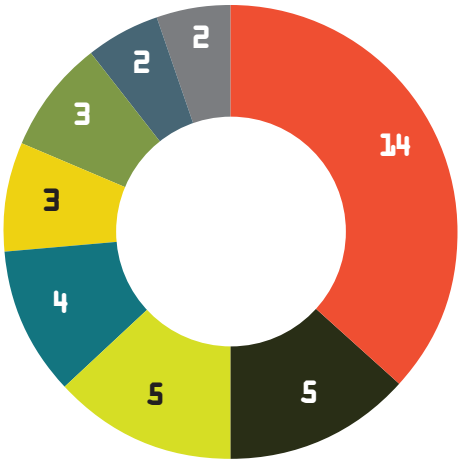
TOP VULNERABILITIES REPORTED SINCE LAUNCH



VULNERABILITIES REPORTED BY MONTH



MOST IMPACTFUL REPORTS SINCE LAUNCH



- CWE-22 PATH TRAVERSAL
- CWE-78 & CWE-77 COMMAND INJECTION
- CWE-284 IMPROPER ACCESS CONTROL & CWE-269 IMPROPER PRIVILEGE MANAGEMENT
- CWE-89 SQL INJECTION
- CWE-200 INFORMATION DISCLOSURE
- CWE-451 USER INTERFACE MISREPRESENTATION OF CRITICAL INFORMATION
- CWE-312 CLEARTEXT STORAGE OF SENSITIVE INFORMATION
- CWE-77 COMMAND INJECTION

2021 / THE YEAR TO BECOME ONE

As we began 2021 with a new pilot on the horizon, VDP made a focused effort to ensure we would work as one with the participants, researchers, and team. Ensuring exceptional collaboration, communication, and understanding not only our researcher but our participants and stakeholders. We wished to reach beyond our comfort zone and make an impact by providing a direct line of communication with all those involved in the pilot. To ensure that our team provided the best service possible, we sent out surveys to collect any feedback and suggestions that would improve the pilot. This led to several one-on-one meetings with the participants, the DIB-VDP Pilot team, and stakeholders to better address concerns for the ever-growing pilot. In addition, the team took extra time with each researcher and participant to explain each issue; this extended to explaining why some tickets could not be accepted, such as Software as a Solution (SaaS). This helped both researchers and participants understand relevancy and the program as a whole. This also pushed the researchers to extend beyond their comfort and encouraged them to submit new tickets ranging in severity. In turn, they gained reputation points, providing them with additional opportunities that extended beyond the DIB-VDP Pilot.

A special thanks to the participants and researchers for continually helping to secure the DOD Defense Industrial Base systems.

LESSONS LEARNED

1. **Scope mix of assets (hostnames, IP and CIDR Blocks) at times makes in-scope validation difficult**
2. **Add DIB partner enhanced report routing protocols to the automated Safety Net**
3. **Baseline Platform for Communication must be in place**
4. **Document formats must be baselined across all stakeholders**
5. **Implement improvements to the on-boarding process to promote scalability**

THANK YOU!

The DIB-VDP Pilot Team would like to acknowledge the support and dedication of our DIB companies, stakeholders, and research partners. Without you, initiating, planning, and executing would have been in vain. Our team has been ecstatic while embracing this opportunity to lead the vulnerability disclosure initiative within the DIB cyber community and forge a new network of partners. Together, we have taken the first step into a new frontier, addressing a neglected essential function of the cyber defense strategy. We recognize the new requirements and custodian responsibility bestowed on us all in this age of rapid technical expansions. This first step has been enormously impactful and crucial to how Cyber defense will be executed in the future. From the front lines, thank you for the collaboration and willingness to move the needle toward a more proactive Cyber defense framework.

"As a DIB-VDP participant, I want to extend my thanks and that of my company for making this pilot available to us. We are grateful and appreciate the service. We have been participating since April 2021. It has been a great benefit. Thank you again."

–DIB Participant Company

DoD CYBER CRIME CENTER AND DEFENSE COUNTERINTELLIGENCE & SECURITY AGENCY

DOD DEFENSE INDUSTRIAL BASE VULNERABILITY DISCLOSURE PROGRAM PILOT

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

"This pilot allowed us to have the confidence to proceed with the AET pilot for penetration testing, which we completed just over a month ago. DCISE has definitely been adding value to the DIB and helping us be prepared and keep pace with emerging threats."

–DIB Participant Company