VULNERABILITY DISCLOSURE PROGRAM

ANNUAL REPORT 2021

VOLUME III

DoD CYBER CRIME CENTER

MESSAGE FROM THE DC3 EXECUTIVE DIRECTOR

WELCOME to the third VDP Annual Report, 2021 Edition!

2021 was a year of distinctive successes for the DOD Vulnerability Disclosure Program (VDP). Each year the DOD VDP Annual Report focuses on unique aspects. The 2019 and 2020 editions highlighted the efforts of the DOD VDP and their stakeholders, respectively. 2021 is a time to reflect on the white hat researchers' positive impact on DODIN. VDP 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.

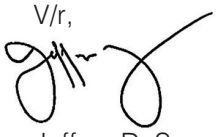
The first milestone of 2021 was the SECDEF issuing the DOD VDP Scope Expansion, which increased the range from only DOD websites to all DOD publicly accessible information systems. The second milestone was the launch of the Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP) Pilot. The jointly executed DC3 and Defense Counterintelligence and Security Agency DIB-VDP Pilot brings the five years of DOD VDP lessons learned to the DIB.

The expansion of in-scope assets for the DOD VDP yielded an average of 979 reports per month to total 11,749 reports for 2021. The ethical hacking community remained vigilant and dedicated to vulnerability discovery by submitting 944 new findings on the 288 DIB-VDP Pilot assets.

White hat researcher continuous engagement and feedback enhances the DOD VDP 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 397 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 commitment of the VDP researchers that bolster the defenses of the DOD's public facing cyber infrastructure.

V/r,



Jeffery D. Specht, SES, DAF
Executive Director
DOD Cyber Crime Center (DC3)

VDP IN GOVERNMENT

1. **National Cyber Strategy**
   a. **Pillar II: Promote American Prosperity**
      i. **Promote Full Lifecycle Cybersecurity**
2. **IoT Cybersecurity Improvement Act of 2020 (H.R. 1668)**
3. **OMB Memorandum M-20-32**
4. **DHS CISA BOD 20-01 and BOD 22-01**
5. **DODI 8531.01 DOD Vulnerability Management**

VDP IN THE NEWS

Ethical hackers continued to fuel VDP in 2021 and in doing so, sometimes made the news. Whether you are interested in the DOD VDP scope expansion, when the VDP director was asked about safe harbor for researchers, or want to learn about the lifecycle of a vulnerability, we have you covered.

You will find VDP articles, podcasts, and more at:
https://www.dc3.mil/News/Vulnerability-Disclosure

EXTERMINATING CYBER BUGS

TEST IT, BREAK IT, FIX IT – REPEAT

2021: The Year of the Researcher

Last year, VDP made a focused effort to ensure we were collaborating, communicating, and understanding our researchers, even more so than usual. Surveys were sent out to top contributors and winners of Researcher of the Month to ask for candid feedback and suggestions that would improve the program and their success. Talks were produced that focused on the researcher community such as Security@ "Incentivizing vs Reacting: Using ROI to Make the Case for Hacker-Powered Security". Analysts took extra time to explain informative issues, or things that could not be accepted such as Software as a Solution (SaaS) issues in some cases. This helped researchers get more comfortable with the triage team as well as the program as a whole to try new things, submit all ranges of severity and bug types and gain reputation for other opportunities. In all with researchers providing the issues, the team was able to mitigate over 6,030 of the vulnerabilities throughout the year. Thank you to the JFHQ-DODIN, the component system owners and of course the researchers for continually helping to secure all publically accessible DOD information systems.

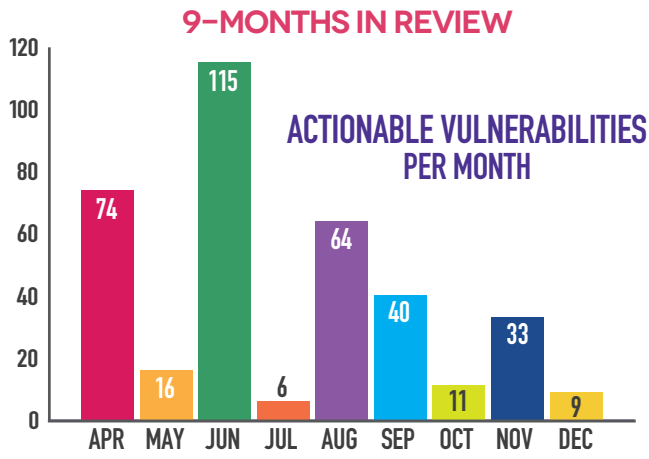
> **"WHAT I LIKE MOST ABOUT WORKING WITH THE DOD TEAM, FEELING THE IMPORTANCE OF WORK WE ARE DOING TOGETHER... [AND] AS I LEARNED MORE, I STARTED TO CONCENTRATE ON HIGH AND CRITS SINCE I WANTED TO DO SOMETHING REALLY IMPORTANT FOR THE SECURITY OF THE DOD, RATHER THAN CREDIT MYSELF. THE FEELING THAT I DID SOMETHING IMPORTANT TO PROTECT ASSETS BELONGING TO THE US FEDERAL AGENCIES WAS A MAIN MOTIVATOR AT THE END."**
>
> —**Sp1d3rs,** White Hat Security Researcher

HUNTING DEFENSE INDUSTRIAL BASE (DIB) BUGS

The 12-month DIB-VDP Pilot provided the five years of lessons learned by the DOD Vulnerability Disclosure Program (VDP) to voluntary cleared and uncleared Defense Industrial Base company (DIBCO) participants. The pilot successfully launched on April 5, 2021, with 14 DIBCOs who chose the 288 assets to put in scope for the crowd-sourced ethical researchers. On a 60-day interval the pilot added new DIBCOs and their assets to expand the protections in the DIB and the supply chain.

The first 9-Months in Review graphic provides the breakdown of the "Actionable Vulnerabilities per Month" 39% of the 944 vulnerability reports submitted by the 247 global researchers were **Actionable**.

For more details see the DIB-VDP Pilot Annual Report at: https://www.dc3.mil/Organizations/Vulnerability-Disclosure/DIB-VDP-Pilot/DIB-VDP-Pilot-Annual-Report/



DOD-VDP: HACKER TESTED, HACKER APPROVED

SCOPE EXPANDED

Our mission is to act as the single DOD focal point for receiving crowd-sourced cybersecurity vulnerabilities on the DODIN to improve network defenses and enhance mission assurance, by embracing a previously overlooked yet indispensable, resource; private-sector white hat researchers. In January 2021, the Deputy Secretary of Defense, expanded the DOD VDP's scope from public facing websites to all publicly accessible DOD Information Systems to include web property, or data owned, operated, or controlled by the DOD. This provides white hat researchers safe harbor to report vulnerabilities over a broader DOD attack surface which effectively reduces outside threats.

Asset types broken out into the following categories: CAC/PKI Protected Assets, Core Network Protocol Misconfiguration, Email/Exchange Server, ICS/SCADA, IoT, Mobile, Network Endpoint, RF, Sensitive Information Exposure, VoIP, VPN, and website/application.

In 2021, after defining asset types and expanding the scope we received 525 reports in a dedicated categories outside of our traditional website/application category used prior to the scope expansion.

PROFESSOR NINA KOLLARS

"In early 2020, I was conducting research for my book on the white hat community, how they operate, and how they create better cybersecurity. In the process, I started to read about VDP and the success of the program for the DOD. One of the unique aspects of VDP is its accessibility. It has to be available to a pretty gnarly, almost feral community of researchers, which means when I reached out to DC3 VDP, and the Director immediately got right back to me. We spent several hours talking about the program, its evolution and growth, and what it is like handling incredibly sensitive information that has the potential to create real problems for US national security. It is one thing for researchers to participate in corporate bug bounty programs and entirely another level what crowd-sourced researchers are doing so for the US Department of Defense. The five-year history of DC3 VDP proves what they are doing works, due to the team's dedication to engaging with the researcher community who secure the DODIN." **—Dr. Nina Kollars**

A very special thank you to Dr. Nina Kollars for visiting the Department of Defense Vulnerability Disclosure Program!

HISTORY OF THE DOD VDP

On 20 October 2016, Secretary of Defense, Ash Carter, signed a memo directing DC3 to lead an internal effort to "bring white hat hackers into the fight to the benefit of the DOD" following the success of the Hack the Pentagon bug bounty pilot. Only a month later, on 21 November 2016, the DOD Vulnerability Disclosure Program (DVDP) launched. Mr. Jon Stivers, DVDP Director, established the "One Team, One Jersey" approach to the unification of effort between DC3, US Cyber Command's (USCC) Joint Force Headquarters DOD Information Network (JFHQ-DODIN) and HackerOne's crowd-sourced white hat hacker community. Five years later, DOD VDP is going strong. Ms. Melissa Vice, Interim Director, is forging the future. The DOD VDP leadership is called upon to provide expert vulnerability disclosure consultation to the White House, Congress, DOD, DOJ, DHS, state governments, 4th estate, academia, cyber committees, private and cleared defense industry.

THE BEGINNING:

20 OCT 2016
Secretary of Defense, Ash Carter signs a memo to empower DC3 to create the DOD Vulnerability Disclosure Program (DVDP)

21 NOV 2016
DC3 established initial operating capability (IOC) for the DOD VDP

NOV 2017
DVDP is renamed DOD Vulnerability Disclosure Program (DOD VDP)

OCT 2018
AMRDEC Safe Access File Exchange (SAFE): Taken offline due to CAC bypass vulnerability

HACKER-POWERED SECURITY

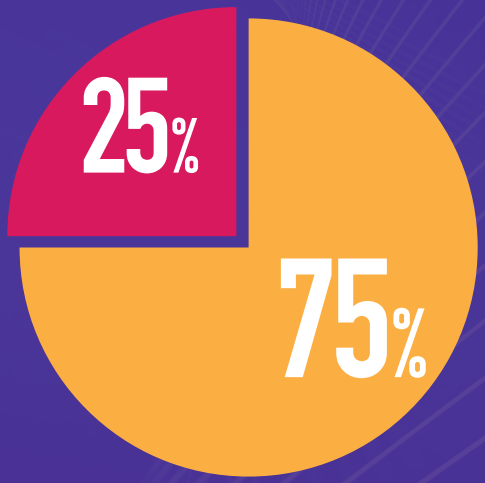
2020 REPORT SEVERITY RATINGS

37,199
VULNERABILITIES SINCE LAUNCH

3,107
RESEARCHERS SINCE LAUNCH

22,030
ACTIONABLE REPORTS SINCE LAUNCH

Total attempted mitigations: 8,054



6,030 Successfully Mitigated Reports
2,024 Unsuccessful Mitigation Attempts

11,749
NEW VULNERABILITIES IN 2021

903
RESEARCHER GROWTH IN 2021

5,585
ACTIONABLE REPORTS IN 2021

RECENT SUCCESSES:

AUG 2019
Pulse Secure VPN: 129 separate critical vulnerabilities reported two days after DEFCON

NOV 2019
Awarded 2019 DOD CIO Team Award for Cybersecurity with a $64M cost-savings from averting cyber-attacks

APR 2020
Federal Voting Assistance Program (FVAP): Discovered 7 critical vulnerabilities that were mitigated to provide election security

15 SEP 2020
DOD VDP and the Vulnerability Report Management Network (VRMN) are included in the **DOD Instruction 8530.01: DOD Vulnerability Management**

APR 2021
DIB-VDP Pilot Launch: 12 Month voluntary pilot to share lessons learned and efficacy of the DOD VDP to DIB companies directly.

JAN 2021
Scope Expansion: DOD VDP policy updated from DOD public-facing websites to all DOD publicly-accessible information systems.

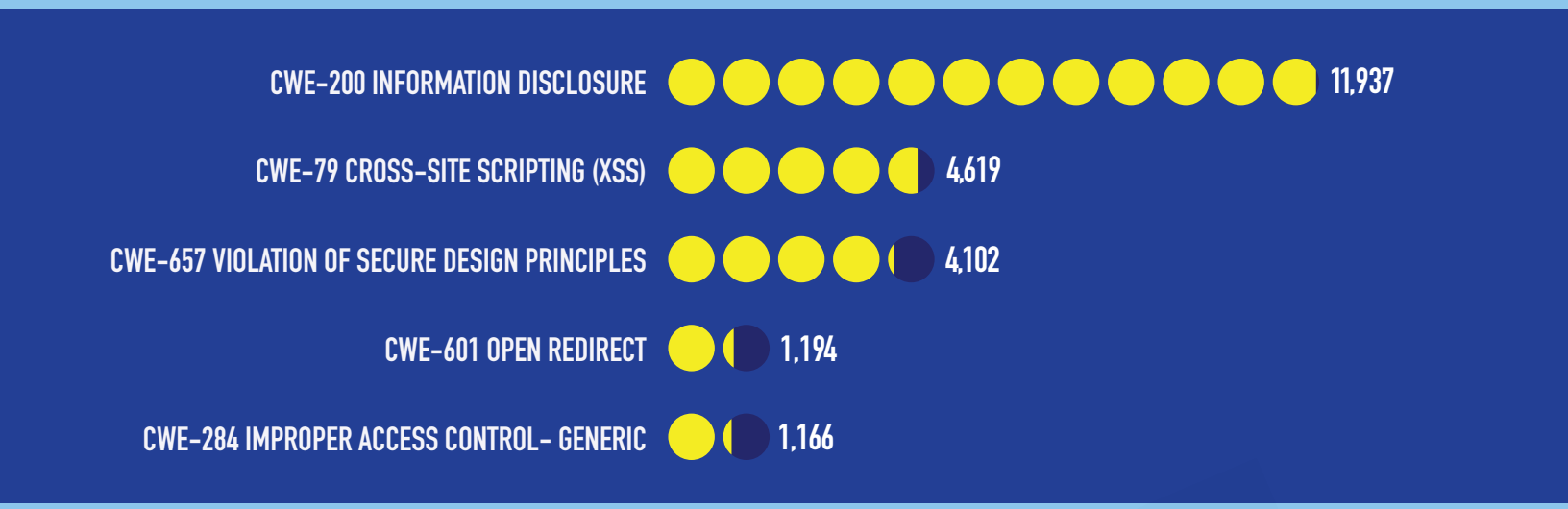
21 NOV 2021
VDP 5th Anniversary

DEC 2021
37,000 Vulnerabilities Received: In under 5 years since the inception of the DOD VDP, white hat security researchers have turned in over 37,000 vulnerabilities to the program.

Focusing on the valuable impact our researchers exhibited by providing critical and high severity vulnerabilities to the DOD, the following are a few brief stories based on some of the large scale and impactful reports that we have received over the past year. With **5,585** actionable reports submitted in 2021, we chose these three to highlight based on your submissions.

CONFLUENCE AT RISK

On August 25th 2021, a critical Object Graph Navigation Library (OGNL) injection vulnerability was published under CVE-2021-26084 affecting Atlassian Confluence servers and data centers. The issue allows for authenticated and often unauthenticated users, to execute arbitrary code on a Confluence Server or Data Center instance. System owners were encouraged to refer to the Atlassian Security Advisory to determine the appropriate fix actions. In total VDP researchers reported 23 of these critical issues, of which half were actionable. Its cases like these where the confluence of VDP and white-hat researchers really makes a difference.

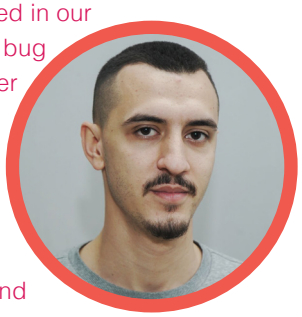


DON'T DOS ME, BRO!

Last year the VDP team got critical reports that a site could be completely taken down with a simple python script. Imagine if an advanced persistent threat (APT) decided to do this with a botnet how much damage could be done. With **36** actionable reports, the DOD got into action, specifically on how their wp-cron.php was configured, when it loaded and how it was being called. Wordpress has listed wp-cron as a feature that can be turned off if desired, but not as an overarching issue. **92%** of all actionable reports submitted were mitigated at the time of writing.

2021 VDP RESEARCHER OF THE YEAR

Drin Ndrecaj better known online as **@drinndrecaj2** or **unknownsh** started reporting to the DOD VDP in May 2021 with a few submissions that were not validated as vulnerabilities and closed as informational findings. He respectfully asked questions, worked with the DOD VDP team and started submitting technical reports that were well written, accurate and of a high quality. Drin went on a hot streak of high and critical severity findings in late June, most of which involving authentication bypasses. These bypasses were not found with default scans or templates but rather required manual testing and exploitation. A few Insecure Direct Object References (IDOR) and some PII leaks in addition to the bypasses earned him the June DOD VDP researcher of the month. Later that same month he also received recognition for reports submitted from the Department of Education. He participated in our DIB-VDP pilot as well as other VDP and bug bounty programs as an active researcher within the community. The DOD VDP is happy to announce that Drin has been selected as the 2021 Researcher of the Year. Through determination, dedication and the willingness to ask questions, the vulnerabilities reported and resolved have saved the DOD time, money and effort. Our team looks forward to what he finds in the upcoming years and wishes him and all our researchers' good luck and happy hunting!



> **"THE DOD VDP IS BY FAR THE MOST RESPONSIVE PROGRAM THAT I'VE EVER ENCOUNTERED ON THE H1 PLATFORM. IT IS THE ONLY PROGRAM THAT CONSISTENTLY RESPONDS TO REPORTS AND ACTUALLY FOLLOWS THROUGH WITH RESOLUTION."**
>
> —**Evilbotnet,** White Hat Security Researcher

HACKED FROM THE EDGE: AN XSS STORY

In 2021 alone, researchers have turned in over 450 Akamai related Cross-Site Scripting (XSS) reports to the VDP. XSS is prominent throughout the web and can be malicious in many ways such as: information disclosure, website defacement; impersonation, etc. This specific issue was directly linked to Akamai Resource Locators (ARL) and allowed for "content not owned by a customer to be served under a customer's 'dangling hostname'." Akamai has listed this as a known issue and as of August 30th started rolling out fixes, pulling us all in from off the edge.

https://community.akamai.com/customers/s/article/WebPerformanceV1V2ARLChangeStartingFebruary282021

DoD CYBER CRIME CENTER

> **“THE ONE THING I LIKE MOST ABOUT THE DOD VDP PROGRAM IS IT'S EXISTENCE! THIS IS ONE OF THE COOLEST DEFENSE PROGRAMS THAT WE HAVE FOR THE DODIN AND SPECIFICALLY NIPR. TAKING INTO ACCOUNT HOW ZERO TRUST AND CLOUD MOVES ARE GOING TO PUT US OUTSIDE THE CAPITAL IAP/JRSS TRADITIONAL DEFENSES, THIS PROGRAM WILL ONLY BECOME MORE IMPORTANT AS A FUNDAMENTAL PART OF OUR DEFENSE METHODOLOGY.”**
>
> —**Warsong,** White Hat Security Researcher