DoD CYBER CRIME CENTER

VULNERABILITY DISCLOSURE PROGRAM 2022 ANNUAL REPORT

VOLUME IV

MESSAGE FROM THE DC3 EXECUTIVE DIRECTOR

WELCOME to the fourth VDP Annual Report, 2022 Edition!

2022 has served as a year marked with significant collaboration for the Department of Defense Cyber Crime Center (DC3) and the DoD Vulnerability Disclosure Program (VDP).

Throughout the year, DC3 has joined our partners from across the DoD and Federal Government in efforts to align cyber defensive vulnerability strategy—with focus on identifying global cyber threats and the subsequent remediation of vulnerabilities. VDP focused its efforts on strengthening our vulnerability mitigation efforts across the U.S. military components and to expand the DoD usage capability of the Vulnerability Report Management Network (VRMN).

Initiated during the onset of the 2020 Covid pandemic lockdowns and the adjustment to virtual normalcy, the DoD VDP has innovated to meet the demand of a nearly 300% monthly increase in cyber vulnerability reporting volumes. VDP recognized our capability to assist DoD system owners with the remediation of such significant vulnerability reporting volumes. Innovations came with increased collaboration with our federal cyber partners and the global ethical researcher community.

2022 included several highly successful collaborations between VDP and our partners, most prominently our partnership with the Defense Counterintelligence and Security Agency (DCSA) to facilitate the Defense Industrial Base - Vulnerability Disclosure Program (DIB-VDP) Pilot. Joint efforts between VDP, DCSA, and the HackerOne research community, resulted in processing over 1000 vulnerability reports. This pilot secured the cybersecurity posture of dozens of voluntary DIB company participants and safeguarding the DIB over $60 million from denied cyber-attacks and exfiltration by potential adversaries.

As the world continues to find its equilibrium and move toward a post-pandemic normalcy, both DC3 and VDP continue to streamline our operating capabilities to a battle rhythm reflective of current cyber threat landscape.

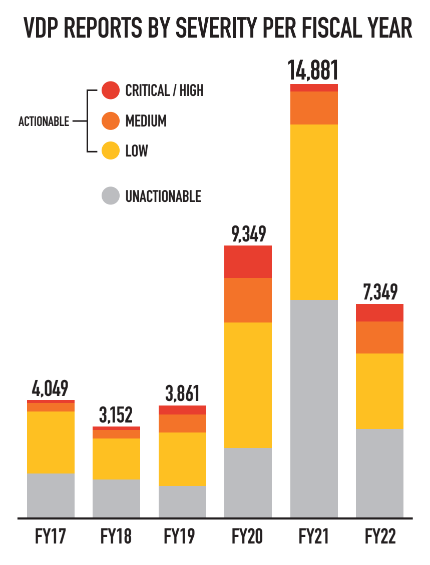
Mr. Jude Sunderbruch, SES, Ph.D
Executive Director
DoD Cyber Crime Center (DC3)

IMPACT OF COVID–19 ON DoD VDP

Prior to the start of COVID-19, DC3's DoD Vulnerability Disclosure Program (VDP) averaged a little more than **300** vulnerability reports a month for a combined total of **11,007** between fiscal years 2017 and 2019. The affect of the global pandemic lockdown was immediately apparent during 2020 with a precipitous rise in reporting volume of **160%** increase that averaged **780** per month in only one year. Fiscal year 2021, resulted in another rise to a staggering monthly average of **1240** reports.

As the world normalized and organizations returned to their former work schedules, the DoD VDP reporting volume reduced to an average of **602** per month in 2022. While still more than **150%** of the pre-covid volume, report totals are within a sustainable battle rhythm and could be subject to further normalization in FY23.

Refer to former VDP Annual Reports for additional annual trend analysis at:
https://www.dc3.mil/Missions/Vulnerability-Disclosure/VDP-Annual-Reports/



DIB-VDP PILOT PROVED

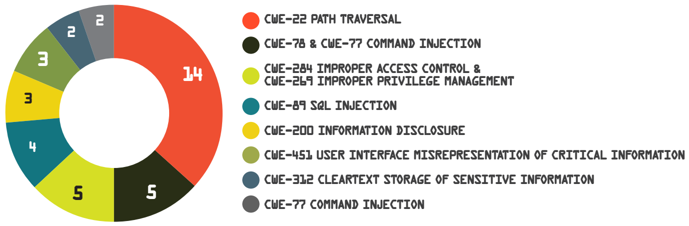
THE DoD VDP MODEL PROTECTS DIB ASSETS

The April 5, 2021 – April 4, 2022 dual sealed Defense Industrial Base Vulnerability Disclosure Program (DIB-VDP) Pilot between DC3 and Defense Counterintelligence and Security Agency (DCSA) provided valuable insights into how the DoD VDP crowdsourced ethical hacker model can be successfully adapted to protect the DIB assets. The pilot focused on a limited number of small and medium sized volunteer DIB companies that wanted to enhance their cybersecurity hygiene and expertise on vulnerabilities. The MITRE ATT&CK framework gives industry adequate mapping for common vulnerabilities and exposures (CVEs), vendor software patches, but does not always map easily to common weakness enumerations (CWEs), often consisting of complex configurations.

The trend analysis of the DIB-VDP pilot revealed the top 10 CWEs and top 15 CVEs closely mirrored the DoD. The DoD VDP with a six-year proven track record and nearly **45,000** documented vulnerability proof-of-concepts and remediations is the natural choice for introducing the defense industrial base to hacker-powered security. The **403** vulnerabilities remediated provided the DIB an estimated $61.4M return on investment from denying cyber-attacks and CUI exfiltration by adversaries.

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

MOST IMPACTFUL REPORTS SINCE LAUNCH



> *"The Vulnerability Disclosure Program (VDP) is complementary to established DoD forward-facing internet vulnerability scan initiatives and assists in protecting NORAD and USNORTHCOM (N&NC) user/systems from current/emerging cyber vulnerabilities. The VDP long-standing effort significantly enhances N&NCs ability to react/respond/report to VDP identified vulnerabilities and is a key component of our overall defense in depth cyber defense strategy."*
>
> —**LCDR Leonard A. DePrisco**, Cyberspace Warning and Operations Center (CWOC) Chief NORAD and USNORTHCOM

2022 DoD CIO TEAM AWARD WINNERS

We are truly honored to be selected amongst a very competitive pool of nominees for the DoD CIO Award for Cyber & IT Excellence in the Teams category. This demonstrates the importance of leveraging the lessons learned from the VDP program to protect the Defense Industrial Base (DIB). The DC3 DIB-VDP team would like to thank the Defense Counterintelligence and Security Agency (DCSA) and our critical partnership with the crowd-sourced ethical researchers. VDP is a team sport and we could not have achieved this level of success without them.

DoD CIO ANNUAL AWARDS WINNER
CYBER & IT EXCELLENCE

General Nakasone, Felicia Barbera, Chiedu Udedibie, John Repici, Joshua Black, Honorable John Sherman, (award recipients not present: Melissa Vice, Damia Sharp, Kristopher Johnson, Ashley Smith, Michael Monroe, Kelly Salisbury, Steve Felmey, Nathanial Joyce, Charles Yarbrough, Krystal Covey, Terry Kalka, Louis Moore, Leah Moore, Gena Brown, Tanya Ortiz, and Terri Cradle.)

SUCCESS THROUGH SHARING

ENGAGEMENT WITH ACADEMIA

On 23 June 2022, U.S. Air Force (USAF), DoD Cyber Crime Center (DC3) signed Cooperative Research and Development Agreement (CRADA) Material Transfer Agreement (MTA) 22-174-DC3-01 with Northeastern University, as Massachusetts Research University, to support two National Science Foundation (NSF) grants obtained to study "Making Security Work: Vulnerability Disclosure Programs (VDPs) and the Organizational Foundation of Cybersecurity." This project directly supports the focus of the Federal Cybersecurity Research and Development Strategic Plan on improving effective and efficient organizational risk management strategies for cybersecurity.

Cybersecurity is now an organizational imperative. High-profile data breaches, ransomware attacks, and other costly exploits and attacks have made cybersecurity a priority for all manner of public and private organizations. Organizations are increasingly adopting vulnerability disclosure programs (VDPs) as a key strategy for managing and mitigating cybersecurity risk. These programs crowd-source security work invite independent security researchers to report newly identified software bugs.

Protecting digital networks, devices,and software is a key national priority. Ultimately, the research project's insights will help organizations improve their security.

Ryan Ellis

Emily Gao

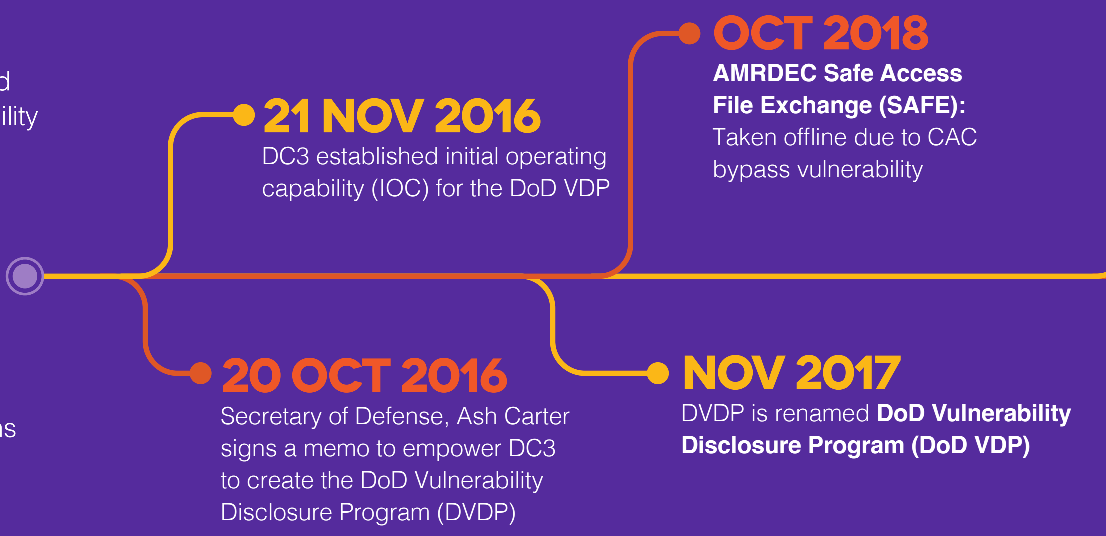
Katie Moussouris

William Robertson

HISTORY OF THE DoD VDP

DC3's DoD Vulnerability Disclosure Program is an enduring operation authorized in 2016 by Secretary of Defense, Ash Carter, and codified in the DODI 8531.01: DoD Vulnerability Management (2020). In 2021, the DoD VDP was issued a scope expansion to all publicly accessible DoD Information Networks and Systems to include Internet of Things (IoT), Industrial Control Systems (ICS), mobile devices, and more further extending the layered defense-in-depth protections by the global crowdsourced ethical hacker community.

ENDURING PROGRAM:



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

BREAKING RECORDS IN VULNERABILITY REPORTING

44,758
VULNERABILITIES SINCE LAUNCH

3,862
RESEARCHERS SINCE LAUNCH

25,762
ACTIONABLE REPORTS SINCE LAUNCH

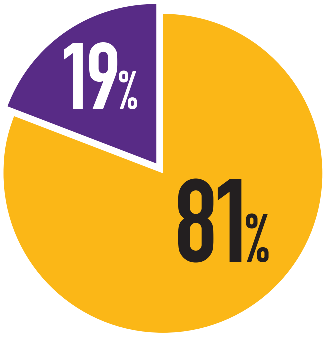
7,349
NEW VULNERABILITIES IN 2022

755
RESEARCHER PARTNERSHIP GROWTH IN 2022

3,838
ACTIONABLE REPORTS IN 2022

TOTAL ATTEMPTED MITIGATIONS

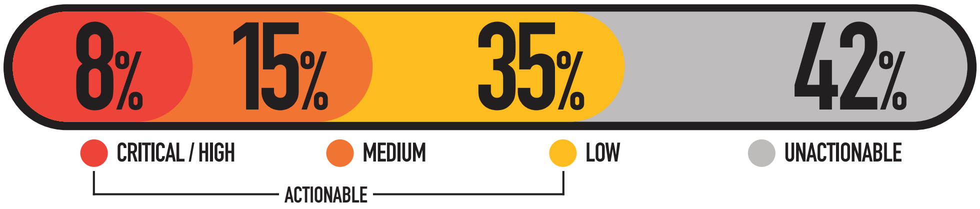
7,827



● 6,346 Successfully Mitigated Reports

● 1,481 Unsuccessful Mitigation Attempts

2022 REPORT SEVERITY RATINGS



RECENT SUCCESSES:

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**

15 DEC 2021
LOG4J Bug Bounty with Defense Digital Service (DDS) for zero-day identification on DoD Information Networks

4 JUL 2022
HACK U.S. Bug Bounty event targeted at critical and high severity vulnerabilities on the DoD Information Networks

9 DEC 2022
Awarded 2022 DoD CIO Team Award for Defense Industrial Base VDP Pilot with $61.4M cost-savings while protecting the DIB

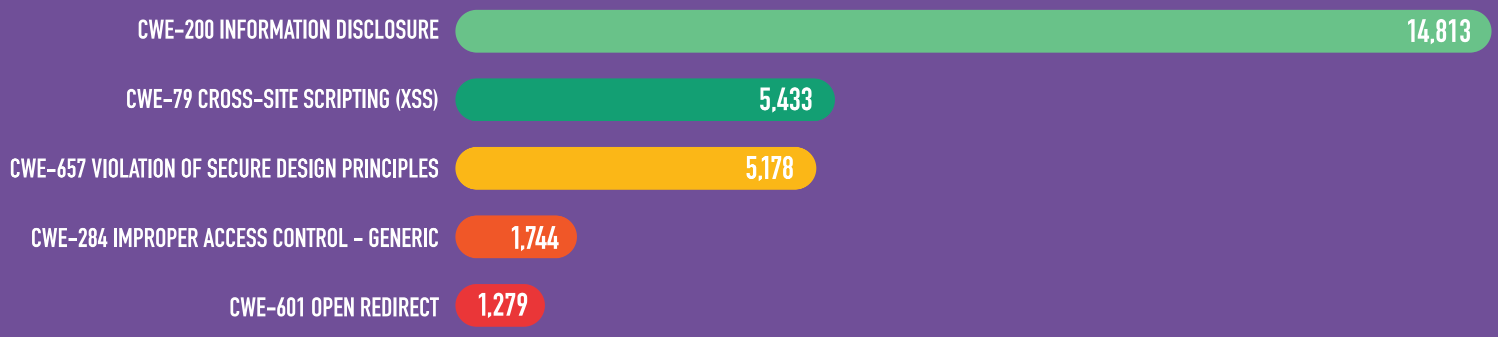
LOG4J IN THE DoD

From mid-December 2021 and into January 2022, the DoD VDP team received multiple submissions regarding the critical Apache Log4J (CVE-2021-44228) vulnerability. Log4J runs on many common services, applications and frameworks. This zero-day's impact and scope was considered potentially large, widespread, and critical within the DoDIN.

DoD VDP in cooperation with the DDS "Hack the DDS" program ran a short bounty for this vulnerability. **77** total reports with **42** of those reports being actionable were submitted over the course of 6 days, all of which were closed as mitigated and resolved within 30 days of triage. DoD VDP received an additional **55** reports after the bounty was run, all of which have been closed and mitigated as resolved. While the total number of findings was relatively small it does not minimize the impact this vulnerability could potentially have had on the DoDIN. Remember to always patch early and patch often.

https://nvd.nist.gov/vuln/detail/CVE-2021-44228 / https://www.cisa.gov/uscert/apache-log4j-vulnerability-guidance

LEADING COMMON WEAKNESS ENUMERATION'S FOR THE YEAR



DC3 IN THE NEWS:

https://www.dc3.mil/News/Vulnerability-Disclosure/

HACK U.S. BUG BOUNTY PILOT

On July 4th, 2022, Chief Digital and Artificial Intelligence Office (CDAO) Directorate for Digital Services (DDS), DoD Cyber Crime Center (DC3), and HackerOne publicly launched the "HACK U.S." bug bounty, allowing ethical hackers from around the globe to earn monetary rewards for reporting of critical and high vulnerabilities from within the DoD vulnerability disclosure program (VDP) published scope. Through piloting the Hack U.S., DoD gains critical insights into how the hacker community competes for prizes with an end goal of strengthening the security of the hundreds of thousands of assets in the DoD scope.

In just seven days, HACK U.S. ethical hackers submitted 648 reports, 349 which were triaged as actionable, resulting in $75,000 in bug bounties and $35,000 in best of category challenge bonuses! The pilot identified how the signal to noise ratio can be reduced by targeting specific severity levels and/or asset ranges; however, participating researchers also submitted another 181 reports that were outside the paid severity range proving the non-monetary reputation points of the "see something, say something" DoD VDP model is enduring.

2022 VDP RESEARCHER OF THE YEAR

M.B. Johnson, also known online as **@deadvolvo** or **maliciousgroup** started reporting to the DoD VDP in September of 2021, submitting several high severity findings. He was very responsive while working with the DoD VDP team submitting vulnerability reports that were well written, accurate, high quality and high impact.

Early in 2022, he found a JBoss Admin panel authentication bypass. In October of 2022, he submitted a critical report for unauthorized file uploads on a DoD asset which could have led to many high-impact attacks, such as Denial of Service via resource exhaustion, credential theft, and command execution. Also, in late 2022 he reported a server with the PUT and DELETE methods enabled, allowing for the upload and removal of files hosted on the server. If this was not remediated, this vulnerability could lead to malicious file execution or web defacement. This report earned him the **October DoD VDP Researcher of the Month**.

In addition, he has also received recognition for reports submitted to the U.S. General Services Administration as well as private sector disclosure programs. He participated in our DIB-VDP pilot and other VDP and bug bounty programs as an active researcher within the community. The DoD VDP is happy to announce that **M.B. Johnson** has been selected as the **2022 Researcher of the Year**. Through determination, dedication, and the willingness to ask and answer 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!

PERFORMANCE STATS 4 1 3

● CRITICAL / HIGH ● MEDIUM ● LOW

> *"The Army's participation in the Vulnerability Disclosure Program is just one mechanism we use to see ourselves and secure ourselves. By leveraging the power and skill of public researchers, we are able to cover much more ground in assessing our network, especially the public facing portion, for critical vulnerabilities that our adversaries may be looking to use to gain an advantage against us in cyberspace."*
>
> —**Lieutenant General Barrett**, Army Cyber Division (ARCYBER) Commander (CDR)

DoD VDP HOSTS FVEY PARTNERS

A very special thank you to Mr. Jonathan Dean and Lt. Col. Adrian Trappett for visiting the Department of Defense VDP.

On 28 July 2022, DC3 VDP hosted the Australian Defence Chief Information Security Officer, Mr. Jon Dean and the Liaison Officer to DISA / JFHQ-DODIN Lieutenant Colonel Adrian Trappett for a dialogue on cybersecurity operations. During this visit, the Aussies received a DC3 Mission Overview and DoD Vulnerability Disclosure Program (VDP) 101 briefing provided by DC3's Acting Executive Director, Mr. Joshua Black and VDP Director, Ms. Melissa Vice.

In addition to hosting the Australians, DC3 has engaged in conversations with other Five Eyes (FVEY) partners about the benefits of a VDP program and how they strengthen the cyber terrain. DC3 looks forward to future collaboration with our allied partners in support of their version of vulnerability disclosure programs.

VDP
CFL
DCISE
DOD CYBER CRIME CENTER
OED
CTA
TSD

> *The Vulnerability Disclosure Program enhanced our vulnerability mitigations for our public facing sites. By identifying essential assets and where to focus efforts to decrease risk, vulnerability management improved our organization's overall security posture. It assisted in limiting threat actors' access to our data and any possible use of it. The VDP program also assisted us in quickly responding to potential threats, enhanced visibility and reporting, kept patching and compliance requirements up-to-date, and facilitated our ability to add operational efficiencies to our organization overall. Over the past year, J341 IDM has overseen and managed the creation of 12 new VDPs and have successfully closed out a total of 27 verified vulnerabilities using the VDP program. These vulnerability categories have ranged from Information Disclosure, Violation of Security Principles, Improper Access Control, Server-Side Request Forgery, Command Injection, Cross-Site Scripting (XXS), and many others.*

—**Brian Borkowski** Chief CGCYBER Compliance and Orders Branch