

UNCLASSIFIED



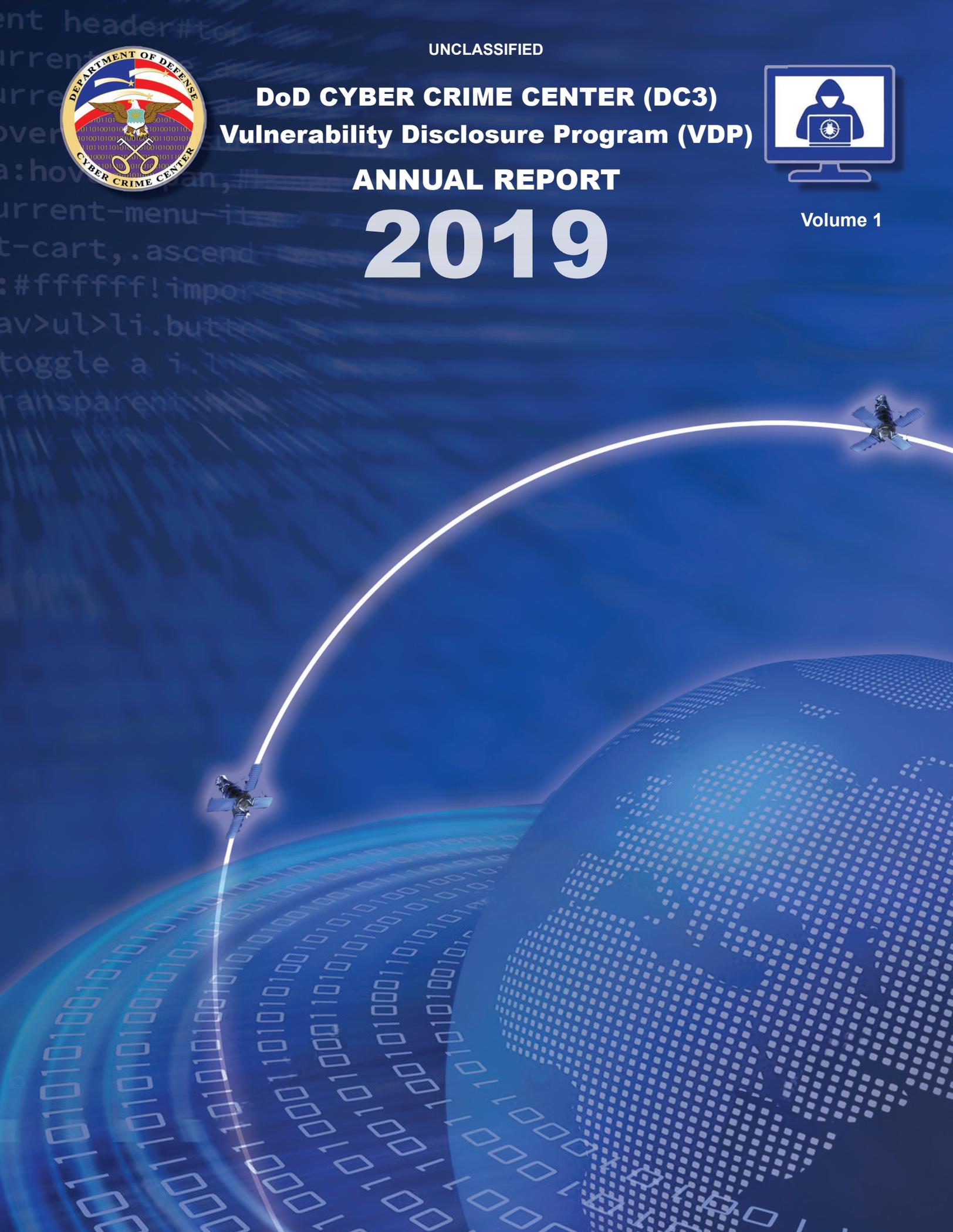
**DoD CYBER CRIME CENTER (DC3)
Vulnerability Disclosure Program (VDP)**



ANNUAL REPORT

2019

Volume 1



Message from DC3 Executive Director

WELCOME to the inaugural VDP Bug Bytes Annual Report, 2019 Edition!

As we reflect on the collective successes of the DoD Vulnerability Disclosure Program (VDP) over the course of 2019, I'd like to first provide a very brief history of the program and how it became a part of the DoD Cyber Crime Center (DC3). Back in the summer of 2016, the Defense Digital Service (DDS) launched the first ever Bug Bounty event for the DoD; Hack the Pentagon. That initial event was so successful that there was an immediate push within the Department to find an avenue to harness the awesome power of the white hat researcher community in a sustained, whole of DoD, 24/7/365 program.

However, up to that point, there was no other Federal agency or legal framework from which to glean lessons learned or best practices, and the size of the Department's attack surface presented complex scoping challenges. Enter DC3, which was selected as the best-suited DoD element to develop the VDP based upon our then 18-year history of supporting cyber operations and our success in launching the equally important DoD Defense Industrial Base (DIB) Collaborative Information Sharing Environment (DCISE) program in 2008. While there have been some inherent growing pains along the way, I am proud to say that in the program's brief 3-year history, the DoD VDP has become both the benchmark and model for the entire Federal Government as well as our international partners looking to develop similar programs. VDP is now so tightly weaved into the DC3 corporate fabric that we are benefiting from the tremendous synergies with DC3's other five directorates; making the DoD VDP and DC3 on whole stronger and more effective.

Again, throughout 2019, the DoD VDP achieved a tremendous number of notable successes. Rather than highlight select vulnerabilities disclosed and mitigated via the VDP, I'd like to take this opportunity to emphasize three essential underpinnings of the program's overarching success: operational impact, partnerships, and process maturity:

- **Operational Impact:** Foundationally, the DoD VDP was established to increase the defensive posture and cyber hygiene of the DoD Information Network (DoDIN). In 2019, they did that by processing a staggering **4,013** vulnerability reports; **2,836** of which were validated and assigned for mitigation. These vulnerabilities were previously unknown to the DoD and not found by automated network scanning software, red teams, manual configuration checks, or cyber inspections. Without DoD VDP there is a good chance those vulnerabilities would persist to this date, or worse, be active conduits for exploitation by our adversaries.
- **Partnerships:** Cybersecurity is a team sport, and VDP would not have been successful without our partners. While this is not by any stretch all-inclusive, I would like to highlight the **1,460** white hat researchers, USCYBERCOM, JFHQ-DoDIN, DDS, Carnegie Mellon's Software Engineering Institute (SEI), and HackerOne. The unity of effort every step of the way has been and remains truly incredible, making clear the value of 'strength in numbers' in aligning the capabilities and talents of multiple partner elements working together to achieve common ends.
- **Process Maturity:** The VDP team deployed several new tools and features to move the program forward, to include: their verified Twitter page @DC3VDP, Researcher of the Month awards, VDP Bug Bytes report, VDP Operating Instruction (OI), and expansion of the Vulnerability Report Management Network (VRMN) platform. The team also spent considerable time consulting with Legislators, the White House, and the Department of Homeland Security on developing language to integrate VDPs throughout the Federal government.

Finally, the icing on the cake for VDP was winning the 2019 DoD Chief Information Officer (CIO) award for Cybersecurity in November. That was no small feat as they competed against 135 other teams in an organization that has almost 3 million employees and one of the largest private networks in the world. Throughout 2019, the VDP had an incredibly positive impact in protecting DoD-wide programs and equities, and I am confident the positive impact of the VDP will only continue to grow in the months and years to come.

Best Regards,



Jeffrey D. Specht, SES, DAF
Executive Director
DoD Cyber Crime Center (DC3)

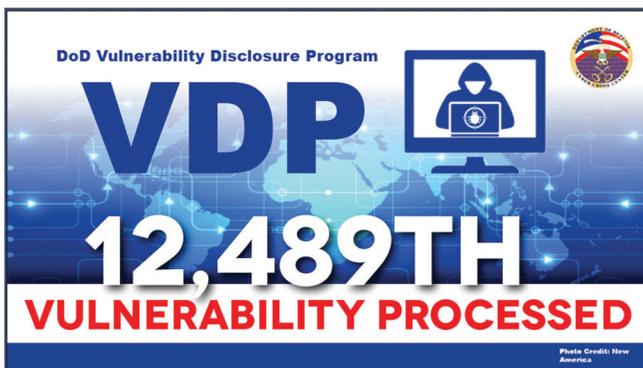


To Infinity and Beyond

While 2019 has arguably been our most successful year to date it is equally important to highlight several of our future goals that we hope will bring great value to the program and the defense of our nation's digital assets. The DoD VDP has developed three distinct lines of effort (LOEs) to strategically drive towards. This allows us to narrow our focus and better align our resources while continuing to provide the same world-class service to the Warfighter.

LOE 1: SCOPE EXPANSION

Our current approved scope limits the researcher's ability to only scan and report vulnerabilities on DoD websites. However, we fully understand that this covers a fraction of the total systems that can be reached from the Internet. Our objective is to take these restrictions off the researchers and allow them to report vulnerabilities they may discover on any DoD information systems. This "See Something Say Something" policy is necessary to cover the entire attack surface today and also include future technologies, services, and protocols.



LOE 2: DEFENSE INDUSTRIAL BASE (DIB) VDP

We have partnered with the Defense Counterintelligence and Security Agency (DCSA) and the DC3 DCISE to perform a 9 month joint feasibility study on what a DoD hosted DIB VDP would look like. We hope to replicate our success by leveraging both the DoD's knowledge and capabilities for private defense companies that do not have the ability or resources to do this on their own. Although it is too early to know, we are excited at the possibility of helping secure the DoD's supply chain.

LOE 3: REPORT ENRICHMENT

The reports that we receive from the researchers contain a tremendous amount of vulnerability information. However, there is more that we can include to better assist system owners downstream who are ultimately charged with mitigating each report. To do that we have partnered with DDS to integrate their internally-developed Crossfeed tool into VRMN so it can automate the inclusion of critical vulnerability data.

Here's to 2020 and the innovation that VDP brings to the fight!

2019 DOD CIO Cybersecurity Award Winners



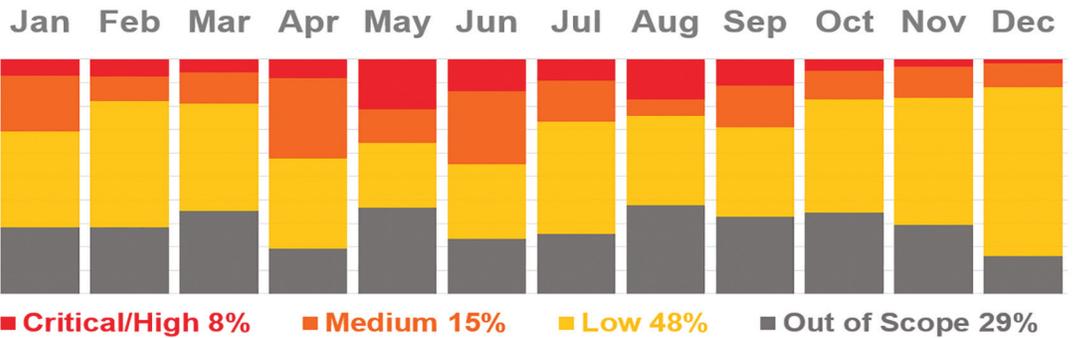
(left to right) Daniel Chatmon, John Stivers, Mr. Dana Deasy (DoD CIO), Chuck Yarbrough, Kristopher Johnson (VDP Director), John Repici, Honorable Karen Evans (DOE), Margaret Mallon (JFHQ-DoDIN), Amanda Rhames, Damia Sharp, Melissa Vice, Tyeshia Long

Vulnerability Report Management Network (VRMN) Metrics

VULNERABILITY REPORTS BY QUARTER



2019 REPORTS SEVERITY RATINGS

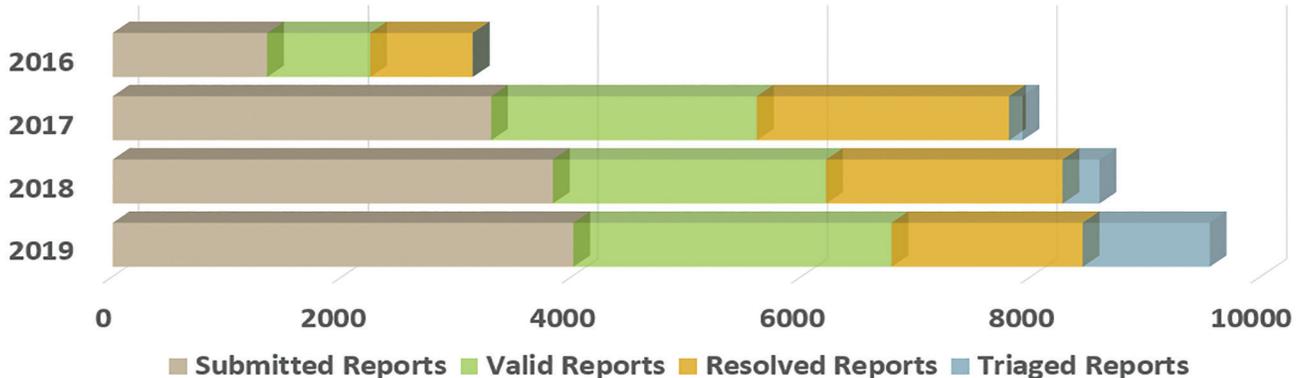


TOTAL SUCCESSFUL MITIGATIONS



This data depicts the number of successful mitigations and validations processed by the VDP team in 2019.

VULNERABILITY REPORTS BY YEAR

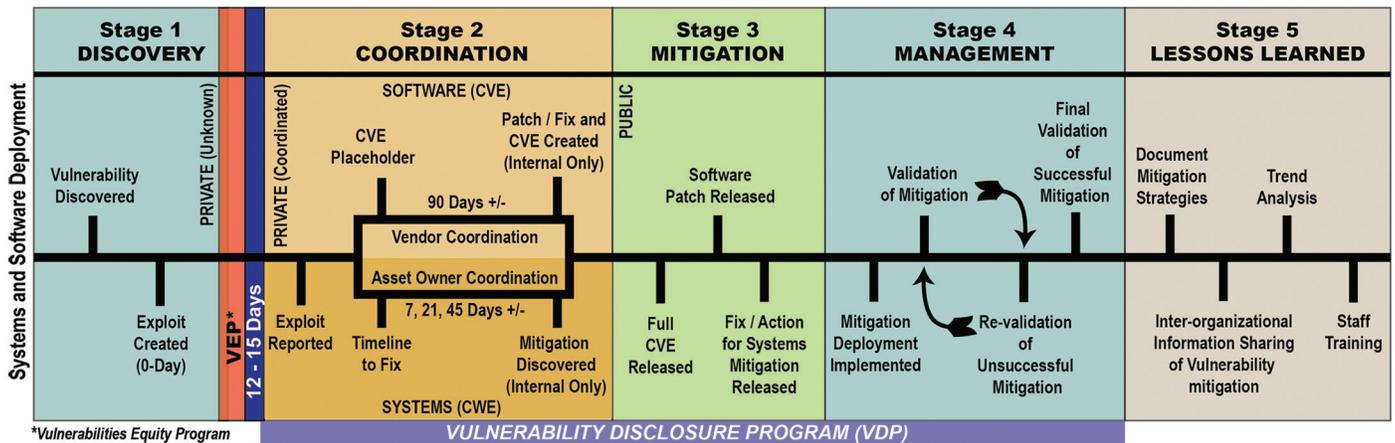


Hacker-Powered Security



The numbers for 2019 don't lie. It was our busiest year to date with a staggering 21.7% increase of submitted reports from 2017. White-hat hackers are improving the DoD's cyber hygiene and driving acceptance of crowdsourcing cybersecurity work in order to more effectively secure our networks. Initiatives like Bug Bounties, VDP, and hacking events like the F-15 at DEFCON this past year, continually demonstrate an unparalleled capability of the researcher community to discover vulnerabilities that our internal DoD agencies haven't. The amazing results cannot be ignored, and we must continue to find ways to partner with the researcher community to illuminate critical DoD information technology system and network vulnerabilities.

Lifecycle of a Vulnerability



THE LIFECYCLE OF A VULNERABILITY IS A FIVE STAGE MODEL: DISCOVERY, COORDINATION, MITIGATION, MANAGEMENT, AND LESSONS LEARNED

DISCOVERY: Just because a vulnerability has been discovered does not mean that it will be exploited. However, for VDP purposes an exploit needs to be created to 'activate' a vulnerability into something that can be acted upon.

COORDINATION: A researcher discloses an exploit proof of concept either through a VDP report, by publishing the exploit to a public source, or incorporating an exploit into an existing research tool or framework so that everyone can use it.

MITIGATION: The mitigation strategy for a vulnerable system is publicly released, either through a vendor-supplied patch or update, or a list of 'fixes' that need to be performed to secure the system.

MANAGEMENT: Once a mitigation for a vulnerability has been released, it is the responsibility of the system owner to deploy and implement the required mitigation. VDPs are used to validate that the mitigation efforts have been performed and are successful on the reported system.

LESSONS LEARNED: The final stage of a vulnerability is to collect, evaluate, and institutionalize the successful mitigations in the form of research reports, trend reports, inter-organizational information sharing, and staff training.

The DC3 VDP process spans Stage 2-Stage 4.

VDP Observations for 2019

IAVA AND RMF COMPLIANCE

The vast majority of vulnerability reports we receive and process are related to misconfigurations in web services and servers. However, we do receive and process vulnerability reports related to unpatched systems and services, servers and software that are either nearing end of life, at end of life or well past end of life. Some of the most severe findings are unpatched VPN endpoints, and we have processed reports for most major vendors; Cisco, Juniper, and Citrix. These tend to be processed as critical findings due to age of the patch level and context of the finding, or in other words part of an information systems security stack and/or endpoint.

VPN endpoints are not the only issue. We also see unpatched and exploitable content management servers

such as DotNetNuke, Wordpress, and even vBulletin with vulnerabilities ranging from simple reflected cross-site scripting and Denial of Service all the way to remote command execution. Always be aware and keep up with released Information Assurance Vulnerability Alerts (IAVA), vendor patch bulletins and make sure to properly configure and update your Assured Compliance Assessment Solution (ACAS).

Following Software/System Development Life Cycle (SDLC), patching and system validation, maintaining hardware and software lists, regularly scheduled vulnerability scanning via ACAS and continuous monitoring of these systems all fall under Risk Management Framework (RMF) requirements.

ALL FLAVORS OF INFORMATION EXPOSURE (CWE-200)

Information exposure is by far the most reported vulnerability processed. This is considered a low severity finding, most commonly information exposure in the response headers from a web server. This particular exposure usually reveals server type and version, php or asp.net version, etc. This is a low severity Security Technical Implementation Guide (STIG) violation which is called out in almost all web server STIGs and Security Requirements Guides (SRGs). Not all information disclosures are equal, but all are preventable. Some reported examples are:

- Improperly reviewed sensitive information exposed in a public server or service.
- Personally identifiable information (PII) and Protected Health Information (PHI) uploaded to a publicly accessible server.
- Unclassified for Official Use Only (FOUO) documents of all kinds as well as export controlled data from third-party contractors.

Make sure all public-facing data is properly redacted with appropriate tools. Ensure data is publicly accessible; make sure this data is behind appropriate authentication mechanisms for accessibility. Make sure your data is properly labeled or there is a disclosure statement on the website; sometimes our analysts aren't sure the validity of the data so we do our due care and diligence and report it. If your data is training material, label it. If the data hosted on your server is intended for public consumption, disclose that in the banner of the website.

Having an info.php file world viewable is a low severity STIG finding. However, in this case there were also credentials; usernames and passwords to not only valid accounts but services as well. These kind of files should never be world viewable and should never have credentials embedded in them. This is no different than putting your username and password on a Post-It under your keyboard. Be aware of STIG requirements and remove or restrict access to certain system files, and never embed credentials of any kind.

2019: YEAR OF THE VPN

2019 was an interesting year, VDP received many VPN submissions. This year showed an enormous uptick over late summer and during Blackhat when a proof of concept was released regarding a Pulse VPN vulnerability and exploit. From mid-August through September, 125 separate reports were processed for this particular finding. In fact, up to the very end of December, VDP and vendors have been very busy. A total of 223 submitted reports were received for VPNs alone.

[CVE-2018-0296 Cisco Adaptive Security Appliance Web Services Denial of Service](#): A vulnerability in the Cisco ASA web interface that would cause a denial of service on the device and effectively force the device to reload. Even though this was first published by the vendor in June 2018, VDP continued to receive valid reports for this vulnerability. We saw an increase in reporting during the month of August and September 2019 when researchers were looking for vulnerable Pulse VPN instances. VDP processed a total of 61 submitted reports for this finding

[CVE-2019-11510 Pulse Secure VPN](#): A vulnerability in the Pulse SSL VPN that could allow a remote arbitrary file to be read with a specially crafted URI that could possibly lead to Remote Code Execution (RCE). The CVE was first published by the vendor in May with a follow-up presentation by the research community demonstrating how to determine if a device was vulnerable. Shortly after that presentation, VDP started to receive a large number of findings within DoD public facing assets. By the time we were done late September, 125 separate reports were processed.

[CVE-2019-19781 Vulnerability in Citrix Application Delivery Controller](#): A vulnerability in the Citrix Netscaler Application Delivery Controller (ADC) that could possibly lead to a remote, unauthenticated actor to perform RCE. This CVE was published late in December with a valid proof of concept following shortly thereafter. As of January 2020, VDP has processed 37 valid findings for this vulnerability.

2019 VDP Researcher of the Year

RESEARCHER BIO:

Sp1d3rs (Eugene Yakovchuk) is a frequent contributor to the DoD VDP and has participated in our program for a number of years. He has also been a contributor to USG TTS Bug Bounty program as well as several of the "Hack the" DDS Bug Bounty programs. He writes fantastic reports and crafts detailed, comprehensive proof of concepts. This year in particular has seen him submit a great many high and critical findings in VPN endpoints found in most of the major VPN vendors. While VDP has had many great participants that have reported critical findings for the DoD and a group of amazing researchers that were awarded "VDP Researcher of the Month" Sp1d3rs contributions this year in helping protect the DoD puts him in a category all his own. We are happy to select him as our Researcher of the Year for 2019!



PERFORMANCE STATS:

35 low severity
72 medium severity
81 critical and high



Since the start of the DoD VDP Sp1d3rs has submitted 355 valid findings; 188 of which submitted in 2019 alone. Everything from open redirects to cross-site-scripting to vulnerable VPN endpoints. Of note, the vast majority of the critical and high findings are all vulnerable VPN endpoints; major vendors to include Cisco, Juniper, and Citrix.

Top 5 Common Weakness Enumerations (CWEs)

For 2019 the following are the top five CWE findings in order as reported to DC3 VDP from the white-hat hacker community. While the vast majority of reports are low to medium severity findings and STIG violations, researchers also turn up higher severity findings. Following STIG and SRG guidance on deployment of new web servers and applications during the lifetime of these technologies through CM control

and continuous monitoring should be a primary focus. Take care of the small things and the big things tend to take care of themselves. The VDP technical team tends to use the Application and Security Development STIG and Checklist as well as all web server STIG/SRGs as a reference. Rarely, if ever do we use any Operating System STIGs when determining validity of findings.

1

CWE-200 (INFORMATION EXPOSURE) - 832 REPORTS

An information exposure is the intentional or unintentional exposure of information to an actor that is not explicitly authorized to have access to that information.

2

CWE -657 (VIOLATION OF SECURE DESIGN PRINCIPLES) - 403 REPORTS

The product violates well-established principles for secure design.

3

CWE-79 (CROSS-SITE SCRIPTING XSS) - 371 REPORTS

The software does not neutralize, or incorrectly neutralizes user-controllable input before it is placed in an output that is used as a web page and served to other users.

4

CWE-840 (BUSINESS LOGIC ERRORS) - 171 REPORTS

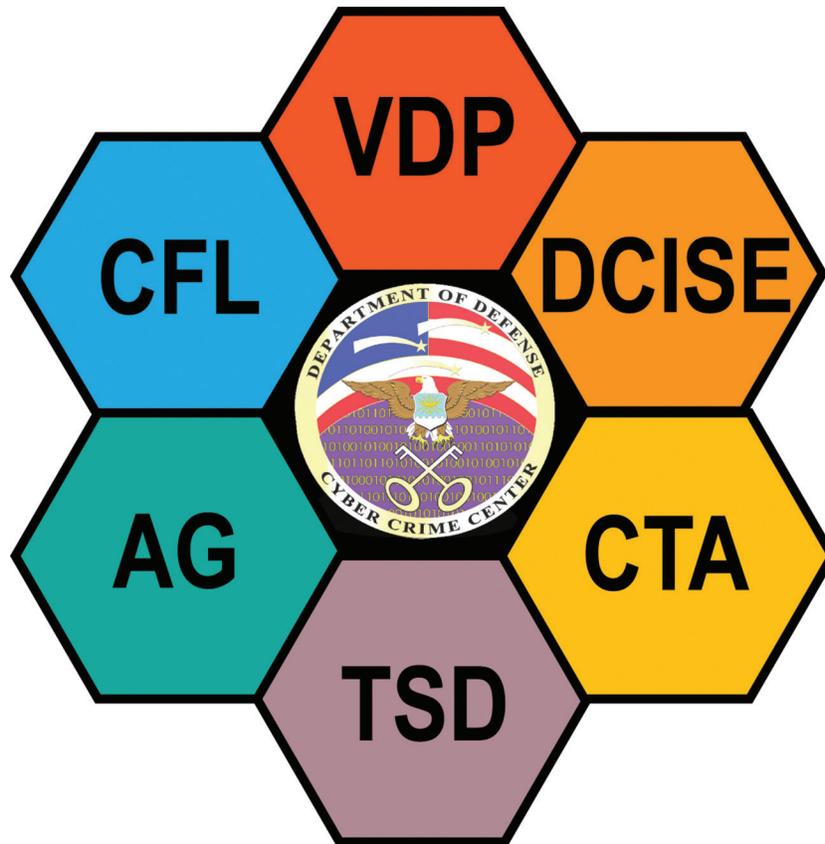
Weaknesses in this category identify some of the underlying problems that commonly allow attackers to manipulate the business logic of an application.

5

CWE-601 (OPEN REDIRECT) - 147 REPORTS

A web application accepts a user-controlled input that specifies a link to an external site, and uses that link in a Redirect. This simplifies phishing attacks.

DC3 Capabilities for DoD Requirements



DOD CYBER CRIME CENTER (DC3) MISSION STATEMENT

Deliver superior digital and multimedia forensic lab services, cyber technical training, vulnerability sharing, technical solutions development, and cyber analysis within the following DoD mission areas: cybersecurity and critical infrastructure protection, law enforcement and counterintelligence, document and media exploitation, and counterterrorism.

Established in 2016 by the Secretary of Defense, the Vulnerability Disclosure Program (VDP) operates to strengthen the security of the Department of Defense (DoD) Information Network (DoDIN) by providing an additional layer to the defense-in depth cybersecurity strategy.

VDP's mission is to act as the single DoD focal point for receiving crowdsourced cybersecurity vulnerabilities on the DoDIN to improve network defenses and enhances mission assurance by embracing a previously overlooked yet indispensable resource; private-sector white hat researchers. The success of the program

relies solely on expertise and support from the security researcher community which contributes to the overall security of the Department.

DoDIN information technologies, services, and systems provide critical capabilities to all military service members, their families, veterans, DoD civilians, and contractors. Ultimately, VDP will drive an increase in the DoDIN's cyber hygiene with the objective of ensuring that the DoD can accomplish its mission to defend the United States of America.

