A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

Bug Bytes—January 2020

DoD Vulnerability Disclosure Program

Mission Brief: The U.S. Government will promote regular testing and exercising of the cybersecurity and resilience of products and systems during development using best practices from forward-leaning industries. This also includes promotion and use of coordinated vulnerability disclosure, crowd-sourced testing, and other innovative assessments that improve resiliency ahead of exploitation or attack.

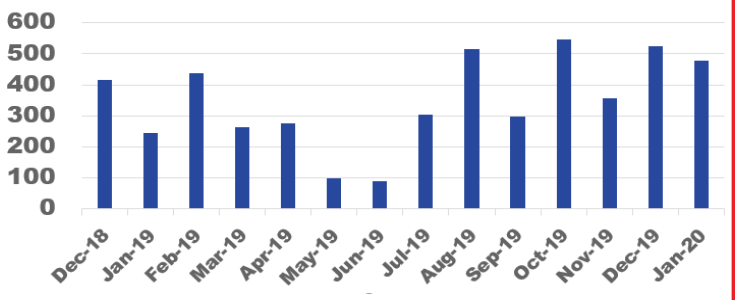
—National Cyber Strategy of the United States of America. September 2018

Knowledge Bytes

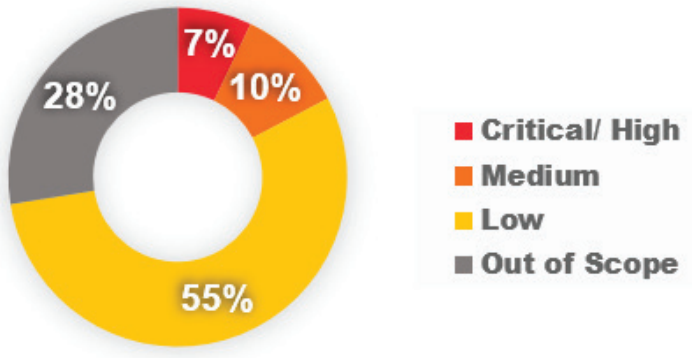
PHP is a popular scripting language that is prevalent in web development and used widely in DoD systems. During the end of January an IAVM (2020-A-0039), listed as a Cat I, was released with upgrade recommendations. The vulnerability is in relation to a buffer overflow that can result in Denial of Service exploitation. There are currently known exploits for this vulnerability, but none are being reported in the wild as of now. Administrators are advised to upgrade their PHP to non-vulnerable versions in compliance with the IAVM. https://iavm.csd.disa.mil/iavm/services/notices/142567.htm

Grand Total Vulnerabilities Since Launch	Total Number of Researchers from Launch	Actionable Reports Processed
13,113	1,500	9,452

New Vulnerabilities Submitted by Month



Severity by Month



Researcher of the Month!

We are excited to start off 2020 by announcing the January 2020 DoD VDP Researcher of the Month Award will go to @p4fg with HackerOne! The researcher submitted 10 critical Citrix findings based on CVE-2019-19781 that could have resulted in a RCE exploit. Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program!

Vulnerability Types

Leading CWE's for the Month	Number of Submissions
Violation of Secure Design Principles	139
Information Disclosure	119
Improper Access Control - Generic	24
OS Command Injection	18
Cross-site Scripting (XSS)	17