A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

Bug Bytes—October 2019

2019 DOD CIO TEAM AWARD WINNERS

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

DoD requires hardware and software lists to be included in all ATO packages as artifacts and uploaded into eMASS. These lists should be updated annually, as needed or as specified by the IAM. Keeping these lists up to date makes keeping your systems patch level current. While missing IAVA only make up ~ 30% of VDP reports, these findings are usually categorized as high or critical findings that could lead to system compromise or loss of availability.

Grand Total Vulnerabilities Since Launch

11,608

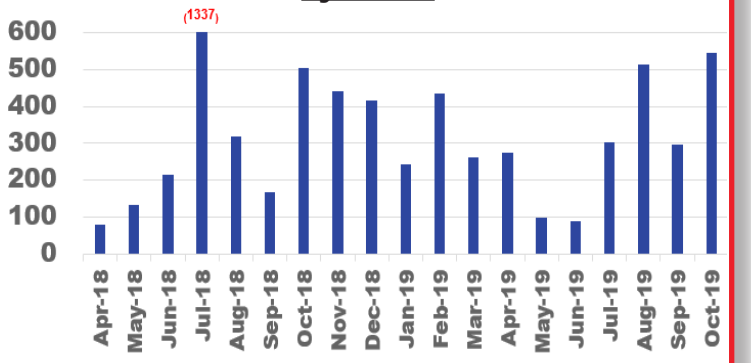
Total Number of Researchers from Launch

1,384

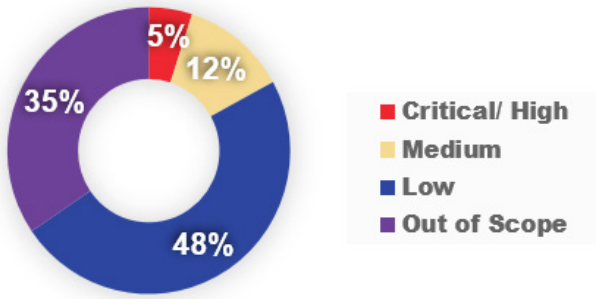
Actionable Reports Processed

8,055

New Vulnerabilities Submitted by Month



Severity by Month



Researcher of the Month!

We are excited to announce that the October 2019 DoD VDP Researcher of the Month Award goes to @brok3npixels with HackerOne! Mukarram's one disclosure exposed MySQL login credentials & other info that would have been harmful if discovered. Congrats and thank you for supporting the DoD!

Vulnerability Types

Leading CWE's for the Month	Number of Submissions
Violation of Secure Design Principles	147
Information Disclosure	141
Cross-site Scripting (XSS)	45
Brute Force	23
Cryptographic Issues- Generic	14