A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

Bug Bytes—AUGUST 2019

2019 DOD CIO TEAM AWARD HONOREES

DoD Vulnerability Disclosure Program

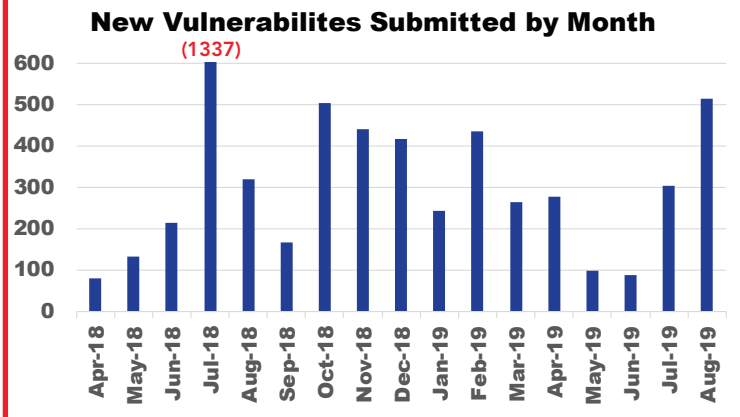
Mission Brief: The U.S. Government will promote regular testing and exercising of the cybersecurity and resilience of products and systems during development using best practices from forward-leaning industries. This also includes promotion and use of coordinated vulnerability disclosure, crowd-sourced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

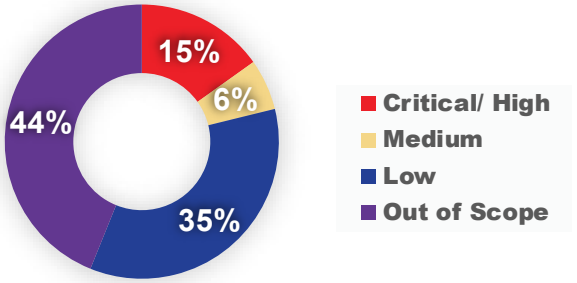
—National Cyber Strategy of the United States of America. September 2018

Grand Total Vulnerabilities Since Launch
10,705
(as of 30AUG2019)

Total Number of Researchers from Launch
1,279

Reduced Triage Time by
86%
(since JULY2018)





Researcher of the Month!

We are excited to announce that the August 2019 DoD VDP Researcher of the Month Award goes to @J3ssie with HackerOne! Not only did this researcher submit 19 validated critical reports for CVE-2019-11510 he also shared his Python script to help us better automate and validate these findings. Great work and kudos for sharing what you made with us and the community!

Vulnerability Types

Leading CWE's for the Month	Number of Submissions
Path Traversal	70
Information Disclosure	60
OS Command Injection	36
Violation of Secure Design Principles	34
Cross-site Scripting (XSS)	26

Top Vulnerabilities Reported

CWE-79	CWE-200	CWE-657	CWE-310	CWE-601
1,959	1,701	1,279	582	502
Cross-site Scripting	Information Disclosure	Violation of Secure Design Principles	Cryptographic Issues	Open Redirect

@DC3VDP

VDP-Questions@DC3.mil