



DoD CYBER CRIME CENTER (DC3) Bug Bytes—SEPTEMBER 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

Knowledge Bytes



In late September Mozilla began gradually introducing a new DNS-over-HTTPS (DoH) capability in the Firefox browser. This is intended to enable users to better secure DNS resolution by encrypting the traffic to and from the browser. More than 70,000 users have already chosen to explicitly enable DoH in their Firefox browser.

Check it out: <https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/>



Grand Total Vulnerabilities Since Launch
11,004
(as of 30SEPT2019)

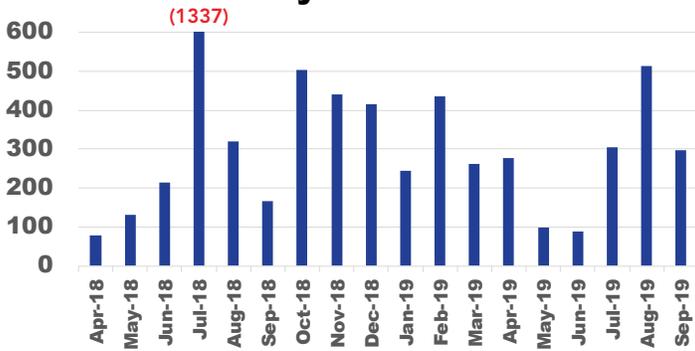


Total Number of Researchers from Launch
1,323

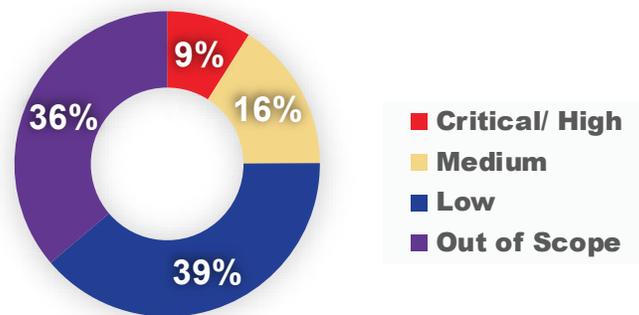


Reduced Triage Time by 86%
(since JULY2018)

New Vulnerabilites Submitted by Month



Total Severity Ratings



Researcher of the Month!

We are excited to announce that the September 2019 DoD VDP Researcher of the Month Award goes to @zok with HackerOne! They submitted a critical RCE vulnerability that would have allowed the enumeration of services, account data and other sensitive info. Congrats and thank you very much!



Vulnerability Types

Leading CWE's for the Month	Number of Submissions
Information Disclosure	105
Violation of Secure Design Principles	39
Cross-site Scripting (XSS)	37
Path Traversal	21
Use of a Broken or Risky Cryptographic Algorithm	16