A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

Bug Bytes—February 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

13,446
Vulnerabilities Since Launch

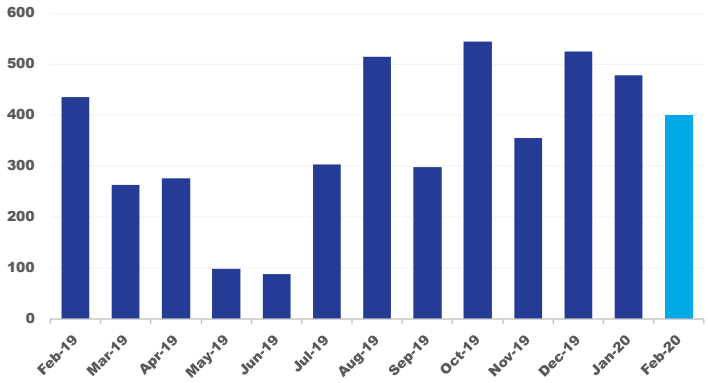
1,541
Researchers Since Launch

9,748
Actionable Reports Processed

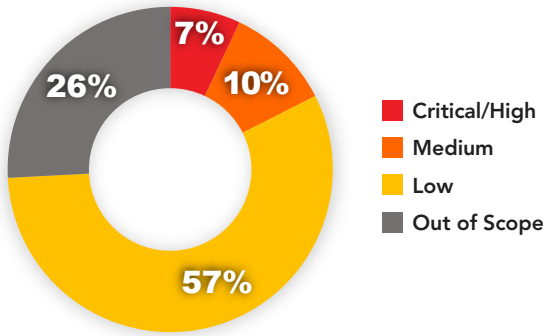
Knowledge Bytes

Apache Tomcat is a widely used servlet and JSP container that is utilized all over the world and implemented throughout the DoD. In February, a read and inclusion vulnerability, that could lead to full Remote Code Execution was released under IAVM 2020-B-0010 (Cat 1). There are multiple different Proof of Concepts in the wild with vulnerable version's dating back 13+ years, making quick mitigation imperative. Patches and upgrades should always be done on a regular basis and in compliance with referenced IAVM's. https://iavm.csd.disa.mil/iavm/services/notices/142621.html

New Vulnerabilities Submitted by Month



Severity for the Month



Researcher of the Month!

The February 2020 DoD VDP Researcher of the Month Award goes to @ngkogkos @hunt4pizza with HackerOne! The researcher reported multiple high and critical vulnerabilities, one specifically allowed privilege escalation as a normal user to an administrator. 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	129
Information Disclosure	106
Business Logic Errors	35
Cross-site Scripting (XSS)	16
Improper Access Control - Generic	16