A FEDERAL CYBER CENTER

DoD CYBER CRIME CENTER (DC3)

Bug Bytes—March 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

13,779
Vulnerabilities Since Launch

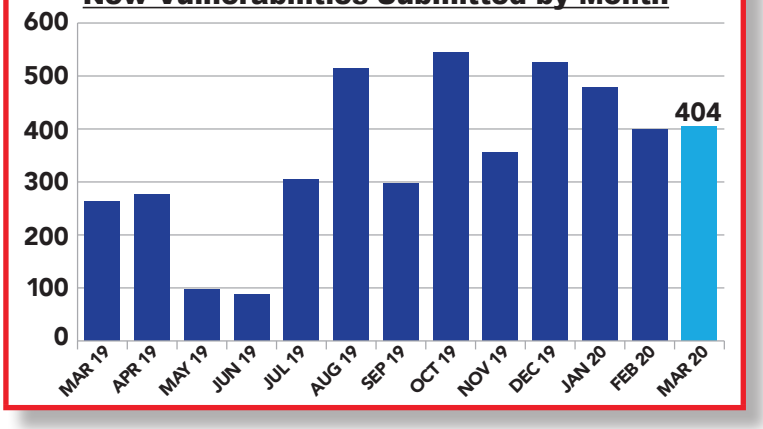
1,570
Researchers Since Launch

10,087
Actionable Reports Processed

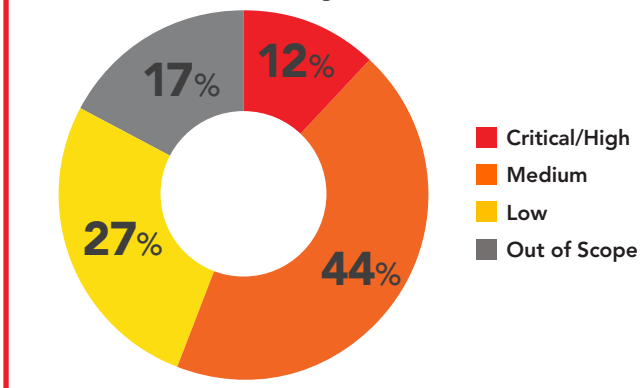
Knowledge Bytes

The Jenkins software, typically used as an open source automation server, has released a security advisory addressing multiple vulnerabilities affecting Jenkins core versions. JFHQ-DoDIN provided 2020-A-0126 (CAT I) notification of how an attacker could exploit these vulnerabilities by enticing a user to open a malicious web page or submit a malicious request to an affected application. DC3 VDP has received reports where this vulnerability is prevalent, as a reminder, these vulnerabilities would allow a remote attacker to gain access to sensitive information, gain unauthorized access, and execute arbitrary code in the context of the affected application. Fix action; apply appropriate Jenkins releases and patch frequently! https://iavm.csd.disa.mil/services/notices/142673.html

New Vulnerabilities Submitted by Month



Severity for the Month



Researcher of the Month!

The March 2020 DoD VDP Researcher of the Month Award goes to @un4gii with HackerOne! The researcher submitted well-written reports that identified various critical and high vulnerabilities including; PII leaks, arbitrary/unrestricted file uploads, and observable sensitive data without authorization. Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program!

Vulnerability Types

Leading CWE's for the Month	Submissions
Information Exposure through Directory Listing	138
Information Disclosure	86
Cross-site Scripting (XSS)	40
Violation of Secure Design Principles	29
Improper Access Control - Generic	10