

DoD CYBER CRIME CENTER (DC3)

Bug Bytes—December 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



WordPress is yet another popular content management system (CMS) used throughout industry and with particularly heavy use within the DoD. A patch was with an accompanying IAVM released towards the end of December (2019-A-0462), listed as a CAT II (moderate severity) with a vulnerability that could allow an attacker to create cross-site scripting attacks (XSS). While there are no known exploits for this vulnerability in the wild, due to the wide spread use of this CMS, administrators as always should patch their servers accordingly and in compliance with the IAVM. <https://iavm.csd.disa.mil/iavm/services/notices/142513.htm>.



Grand Total Vulnerabilities Since Launch

12,489



Total Number of Researchers from Launch

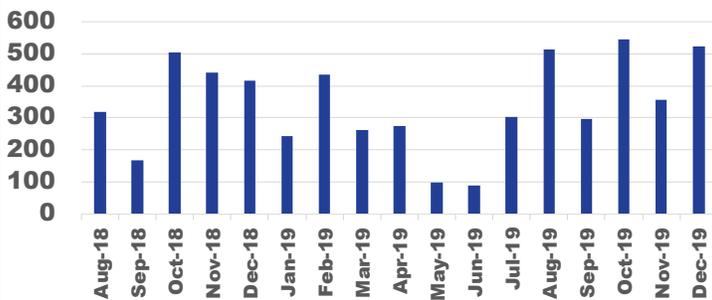
1,460



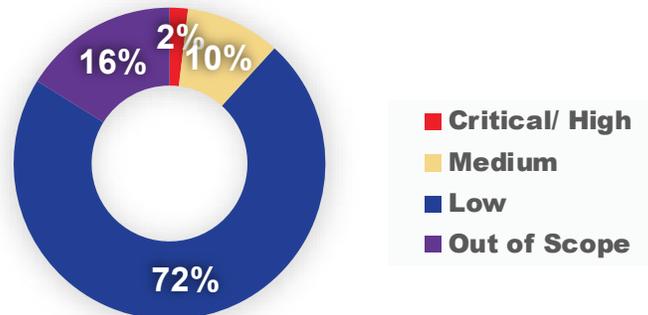
Actionable Reports Processed

8,994

New Vulnerabilities Submitted by Month



Severity by Month



Researcher of the Month!

Happy Holidays #Hackers! We are pleased to announce that the December 2019 DoD VDP Researcher of the Month Award goes to @al-madjus with HackerOne! The researcher submitted a critical severity finding on a DoD website that would allow the disclosure of account credentials of database users as well as other sensitive information about the server itself. Awesome find and thank you for participating in the DoD Vulnerability Disclosure Program!



Vulnerability Types

Leading CWE's for the Month	Number of Submissions
Information Disclosure	221
Violation of Secure Design Principles	147
Cross-site Scripting (XSS)	32
Cryptographic Issues	25
Memory Corruption	24