DOD VULNERABILITY DISCLOSURE PROGRAM

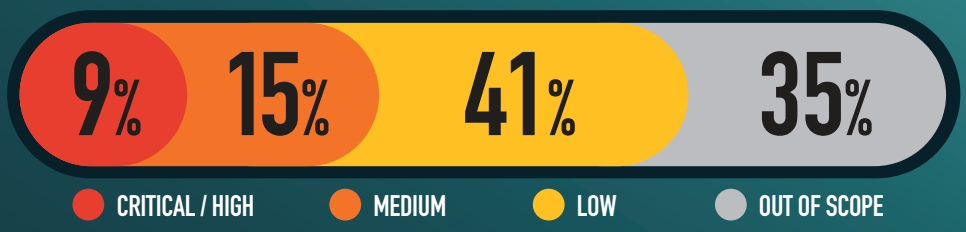
BUG BYTES JUNE 2020

15,705
VULNERABILITIES SINCE LAUNCH

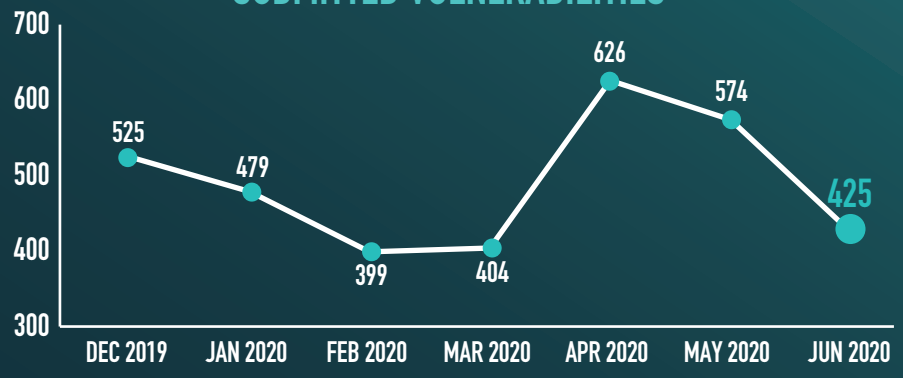
1,756
RESEARCHERS SINCE LAUNCH

11,198
ACTIONABLE REPORTS PROCESSED

SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING CWE'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE	117
CWE-284 IMPROPER ACCESS CONTROL - GENERIC	48
CWE-79 CROSS-SITE SCRIPTING	40
CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES	35
CWE-209 INFORMATION EXPOSURE THROUGH AN ERROR MESSAGE	30

KNOWLEDGE BYTE

A critical patch was released in early June for a Windows SMB Authenticated Remote Code Execution vulnerability as notice number 2020-1301. If an attacker successfully exploits the vulnerability, they could gain the ability to execute code on the target server. Please update as soon as possible! Further information is available at https://iavm.csd.disa.mil/iavm/services/notices/142791.htm

RESEARCHER OF THE MONTH

The June 2020 DoD VDP Researcher of the Month Award goes to **@W3ld35u5W (aka Un]{n0wn, un_kn0wn)** who joined us last month on HackerOne! The researcher discovered one critical and three high serverity findings that ranged from Access Control manipulation, Session Token capturing, and RCE. Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program!

@DC3VDP
VDP-Questions@DC3.mil

DC3 DOD CYBER CRIME CENTER