

BUG BYTES

OCTOBER 2020



22,566

VULNERABILITIES SINCE LAUNCH

2,048

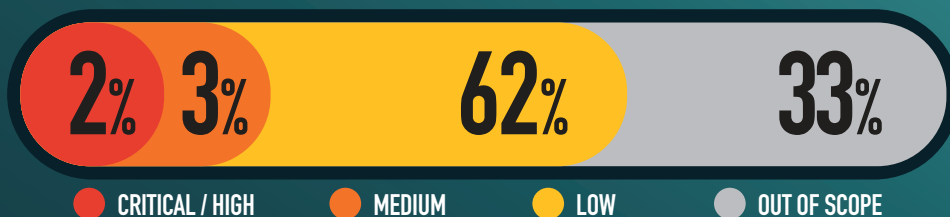
ALL-TIME RECORD!

RESEARCHERS SINCE LAUNCH

15,233

ACTIONABLE REPORTS PROCESSED

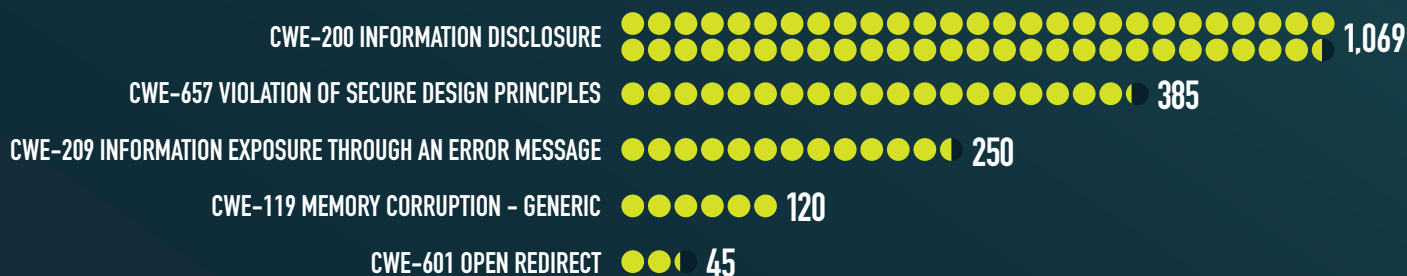
SEVERITY FOR THE MONTH



SUBMITTED VULNERABILITIES



LEADING CWE'S FOR THE MONTH



KNOWLEDGE BYTE

Our team continues to see vulnerabilities, submitted by our researchers, which highlights a weakness in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software. CVE-2020-3187 could allow an unauthenticated remote attacker to conduct directory traversal attacks. Additionally, it could provide the capability to manipulate authorizations to sensitive files on a targeted system. Nefarious actors are only able to view and delete files within the web services file system. At this time, Cisco has released software updates that address this vulnerability. The vulnerability is due to a lack of proper input validation of the HTTP URL. Further information is available at: <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2020-3187> & <https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-path-JE3azWw43>

RESEARCHER OF THE MONTH

We are happy to announce the October 2020 DoD VDP Researcher of the Month Award goes to [Jeff Steinburg @SilentBreach](#) who joined us last month for the first time on HackerOne! The researcher submitted both high and critical severity findings, the IDORs reported allowed for unauthorized information disclosure and unauthenticated account takeovers. Keep up the great work and thank you for participating in the DoD Vulnerability Disclosure Program! Happy Hacking!

