

## BUG BYTES NOVEMBER 2022



44,463

VULNERABILITIES SINCE LAUNCH

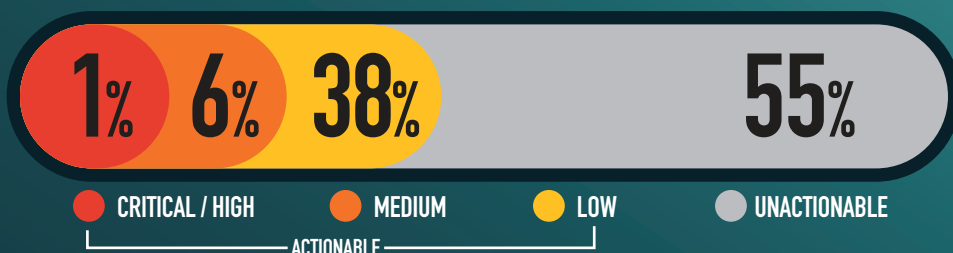
3,832

RESEARCHERS SINCE LAUNCH

25,559

ACTIONABLE REPORTS PROCESSED

## SEVERITY FOR THE MONTH



## SUBMITTED VULNERABILITIES



## LEADING COMMON WEAKNESS ENUMERATION'S FOR THE MONTH

CWE-200 INFORMATION DISCLOSURE ●●●●●●●●●●●●●●●● 115

CWE-284 IMPROPER ACCESS CONTROL - GENERIC ●●●●●●●● 42

CWE-657 VIOLATION OF SECURE DESIGN PRINCIPLES ●●●● 26

CWE-79 CROSS-SITE SCRIPTING (XSS) ●●● 20

## KNOWLEDGE BYTE

In November 2022, a researcher was able to provide a proof of concept exploiting outdated DNS records, which pointed to a decommissioned webserver. This allowed them to register their own service at that decommissioned IP endpoint and was then able to obtain an SSL certificate from a commercial 3rd party issuer, lending further credibility to the controlled host. It is recommended that system owners continually evaluate their DNS footprint, including subdomains, and adhere to a robust system lifecycle process for all name resolution services and certificates. See the following for more information:

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf>

<https://arxiv.org/pdf/2204.05122.pdf>

## RESEARCHER OF THE MONTH

The DoD VDP Researcher of the Month for November 2022 is [@corrie\\_sloot!](#) They submitted a critical report for a subdomain takeover on a DoD asset that could lead to an attacker gaining control of a targeted domain. Thank you very much! VDP Hackers for the win!