TLP:CLEAR

VDP PLATFORM BUG BOUNTY FACT SHEET

WHAT IS A BUG BOUNTY?

A bug bounty provides financial incentives to public security researchers to invite them to search for, discover, and report vulnerabilities in specific systems. Bug bounties provide an efficient and rewarding method for federal civilian executive branch (FCEB) agencies to engage with researchers who may be able to identify vulnerabilities in specific systems before they are exploited by adversaries.

Bug bounties are an optional feature of the Cybersecurity and Infrastructure Security Agency (CISA) Vulnerability Disclosure Policy (VDP) Platform and are not required by Binding Operational Directive (BOD) 20-01. Agencies determine the payment amount and fund the rewards (i.e., the bounty). The VDP Platform then facilitates the agency-funded payment to the researcher.

HOW THE VDP PLATFORM SUPPORTS BUG BOUNTIES

The bug bounty functionality enables agencies to take full advantage of the VDP Platform's vulnerability management offerings. The VDP Platform assists agencies in maximizing the bug bounty functionality in several ways, including:

- Supporting agencies' ability to intake, triage, and track remediation of vulnerabilities.
- Facilitating and tracking bounty payments to researchers, based on agency-defined bug bounty policies.
- Supporting agencies in developing the scope and "Rules of Engagement" for the bug bounty.
- Supporting agencies in establishing and publicizing a market-competitive bounty table.
- Promoting the agency bug bounty launch to the researcher community through CISA's communication channels and the VDP Platform.
- Providing agencies access to a pool of highly skilled researchers, vetted through a background check process.
- Helping agencies with managing the researcher community by determining the best researcher pool, establishing researcher criteria, verifying identification, and managing communication efforts.

BUG BOUNTY TARGETS, TIMELINES, AND AWARDS

CISA's VDP Platform enables agencies to customize different aspects of their bug bounty programs. Agencies have the option to set up a private bounty program with a select number of highly skilled, vetted researchers. Agencies determine the number of systems to be tested during the event and the budget (i.e., bounty pool) to incentivize testing.

Vulnerabilities are triaged for impact and categorized by their severity type (P1 to P5). Payouts made to researchers are correlated to the severity score of the submitted report (i.e., critical vulnerabilities are issued higher payouts than moderate vulnerabilities). Once bounty pool funds are depleted (or the testing period ends), the bounty-associated testing window closes.

VDP PLATFORM BUG BOUNTY PILOT

Leveraging the VDP Platform, the Department of Homeland Security (DHS) launched the Hack DHS pilot event, a crowd-sourced bug bounty that incentivized the researcher community to search for vulnerabilities in certain DHS systems.

Over three separate phases, ranging from December 2021 to February 2023, top researchers from around the world participated and disclosed vulnerabilities on DHS systems. These uniquely skilled researchers identified vulnerabilities that traditional testing methods missed. As DHS Secretary Alejandro Mayorkas announced in 2023, Hack DHS led to the successful identification and mitigation of vulnerabilities, including one that would have allowed individuals to bypass security on the department's official .gov site, potentially allowing malicious hackers to send official communications from department email addresses. If exploited, this vulnerability could have caused serious consequences, including potentially interfering with department communications and negatively impacting public trust in DHS. The vulnerability was discovered and addressed thanks to one of the more than 500 researchers participating in Hack DHS.

Hack DHS demonstrated that agencies already using the VDP Platform could activate the platform's bug bounty capability swiftly and effectively. The pilot successfully laid the path for how federal agencies could leverage bug bounties as part of handling vulnerability management across a federated environment, triaging vulnerabilities rapidly and swiftly connecting with agency technical teams for remediation. Since Hack DHS, the VDP Platform has helped other agencies establish bug bounty programs as well.

For more information, visit CISA's CISA's VDP Platform page or contact Cybersharedservices@mail.cisa.dhs.gov.