VULNERABILITY DISCLOSURE POLICY PLATFORM FACT SHEET

August 2022

BACKGROUND

The Cybersecurity and Infrastructure Security Agency (CISA) established the Vulnerability Disclosure Policy (VDP) Platform to improve the security of federal agencies' internet-accessible systems through a centrally managed vulnerability intake system. The VDP Platform was fully authorized to operate in March 2022 and has since furthered:

- Binding Operational Directive (BOD) 20-01, which requires agencies to develop and publish a VDP;
- BOD 22-01, which focuses on reducing the risk of known exploited vulnerabilities (KEVs); and
- Executive Order (EO) 14028, "Improving the Nation's Cybersecurity," which seeks to improve agency vulnerability management capabilities, among other goals.

PURPOSE

The VDP Platform promotes good faith security research to achieve improved security and coordinated disclosure across the federal civilian enterprise. The VDP Platform also improves vulnerability detection on federal networks by enabling participating agencies to benefit from timely reporting that, in turn, facilitates prompt remediation. Finally, the VDP Platform helps agencies comply with EO 14028 by generating greater agency user awareness of existing vulnerabilities.

FUNCTIONALITY

CISA's VDP Platform provides a primary entry point for vulnerability reporters and alerts participating agencies to potential issues on federal information systems. At a high level, the service:

- Screens spam and performs base-level validation on submitted reports.
- Flags vulnerabilities and links reports that are related by vulnerability type, reporter, and more.
- Provides a web-based communication mechanism between reporter and agency.
- Allows users to create and manage role-based accounts for their organization and suborganizations.
- Offers an application programming interface to take various actions on vulnerability reports, such as pulling reports into agency ticketing systems.
- Delivers reporting metrics, minimizing agency burden in complying with BOD 20-01's requirements.
- Alerts reporter and agency users on updates from CISA, based on events of interest and metrics approaching or hitting defined thresholds.

VALUE

CISA's VDP Platform offers several benefits for its users, including:

- **Compliance With Federal Requirements:** CISA centrally manages the VDP Platform, ensuring compliance with government-wide standards, policy, and business requirements.
- **Reduced Agency Burden:** CISA hosts the VDP Platform, manages administrative responsibilities, and provides user management and support. The service includes initial triaging related to validity, which assists with timely validation of reports.
- **Improved Information Sharing Across Federal Civilian Enterprise:** By enabling CISA to maintain insight into disclosure activities, the VDP Platform improves information sharing across the federal civilian enterprise. Data from the platform has now been incorporated into CISA's vulnerability management products, such as its Insights reports.
- **Automated KEVs Support:** The VDP Platform facilitates agency compliance with BOD 22-01 by providing automated support to help agencies match submissions with KEVs in the CISA-managed Known Exploited Vulnerabilities Catalog.
- **Centralized Access Point for Researchers:** Participating agencies can choose to host their VDP on the vendor's website, generating increased visibility and public researcher engagement opportunities.
- **Automated Metrics and Reports:** The VDP Platform automatically generates reporting metrics to satisfy BOD 20-

01 requirements and submits these on behalf of the agency. The service further alleviates reporting burdens by automatically generating the following metrics:

- Number of valid reports
- Number of currently open and valid reported vulnerabilities
- Median age of open and valid reported vulnerabilities
- Median age of reports older than 90 days
- Number of currently open and valid vulnerabilities older than 90 days from report receipt
- Number of all reports older than 90 days, sorted by risk/priority level
- Time needed to validate and mitigate submitted vulnerabilities and reports
- Time needed to initially respond to the reporter

ROLES AND RESPONSIBILITIES

CISA's VDP Platform is a software-as-a-service application designed to alert participating agencies about issues on their internet-accessible systems. However, vulnerability remediation on federal information systems will remain the responsibility of the agencies operating those networks. A breakdown of roles is as follows:

- **Vulnerability Reporters:** Utilize the VDP Platform as a central place to report vulnerabilities in federal systems of participating agencies.
- **Platform Vendor (EnDyna/Bugcrowd):** Provides screening and initial triage to validate vulnerabilities.
- **CISA:** Maintains insight into disclosure activities but does not actively participate in disclosure remediation processes. (CISA will have read-only access to all agency reports to view aggregate statistical data and reports.)
- **User Agency:** Maintains a separate profile in the VDP Platform. By logging into the platform's interface, users can see an agency dashboard with a list of submissions and general statistics.

SIGN-UP

CISA will fund all costs associated with the platform through February 2025. The platform is free to all federal civilian executive branch agencies that fall under CISA's authorities. CISA will work with agencies to configure VDP Platform service in response to their requests. Any agency interested in participating or receiving additional information should contact vdpplatform@cisa.dhs.gov.