Edgesource's Cybersecurity Virtual Learning Environment (CVLE) Vulnerability Disclosure Program (VDP) Policy And Rules of Engagement (ROE)

Version 1.0
June XX, 2023

CONTENTS

This document is adapted from the Vulnerability Disclosure Program (VDP) Policy and Rules of Engagement (ROE) from DHS 4300-A Sensitive Systems Handbook.

1.0 PURPOSE

In accordance with Section 101 and Title I of the SECURE Technology Act (P.L. 115-390), this policy provides security researchers with clear guidelines for (1) conducting vulnerability and attack vector discovery activities directed at the CVLE and (2) submitting those discovered vulnerabilities. This policy has been developed to satisfy Cybersecurity and Infrastructure Security Agency's Binding Operational Directive (BOD) 20-01, *Develop and Publish a Vulnerability Disclosure Policy* and to improve the cybersecurity of the CVLE.

2.0 OVERVIEW

Cybersecurity Virtual Learning Environment (CVLE) is a web-based platform developed by Edgesource Corporation to deliver cybersecurity training at the request of and in support of the Academics Branch of the Cybersecurity Infrastructure and Security Agency (CISA) within the Department of Homeland Security (DHS). The purpose of CVLE is to have a platform to meet the expanding online learning requirements to deliver web-based, on-demand courses with hands-on lab components. CVLE is hosted in an Amazon Web Services (AWS) GovCloud region and is operated as a Software-as-a-Service (SaaS).

The CVLE has three components;

- Landing Page
- Learning Management System (LMS)
- Cyber Range.

The Landing page is an identity-aware static website to provide students with the course catalog's training opportunities. The LMS is based on the Moodle open-source learning platform and provides

student registration, tracking, and content management. The Cyber Range is a secure platform that provides simulated networks and applications in a safe environment for students to participate in hands-on activities and learning.

As part of the CVLE Authority to Operate (ATO) and continuous security improvement, Edgesource recognizes that security researchers regularly contribute to the work of securing organizations and the Internet as a whole. Therefore, Edgesource will accept and review properly submitted reports of any vulnerabilities discovered within the CVLE or its associated websites[1]. Information submitted under this policy will be used for defensive purposes to mitigate or remediate vulnerabilities in this system.

Hereinafter, researcher[2] may be referred to as "you" or "your" and Edgesource may be interchangeably used in conjunction with or alternatively referenced as "we", "our", or "us".

3.0 SCOPE

This policy applies to the CVLE system, application, or associated infrastructure used, operated, or controlled by Edgesource.

This policy applies to all domains and subdomains of https://www.edgesource-training.com as belonging to Edgesource Corporation.

4.0 HOW TO SUBMIT A REPORT

Edgesource Corporation follows RFC 9116 and implements a security.txt mechanism as approved in CISA BOD 20-01. The contents of this file include, but are not limited to the following:

- Contact Information
- Preferred Language(s)
- Link to Relevant Security Policy
- PGP Encryption Information
- Canonical URL Information

Using the above contact information, please submit a report of the vulnerability (a “Vulnerability Report”). An example of the Vulnerability Report would include a detailed summary, including:

- Type and description of vulnerability
- FQDN, IP Address or hostname
- Instructions to replicate
- Applicable evidence
- Potential impact to system/site
- Recommended remediation actions

5.0 GUIDELINES

By submitting a Vulnerability Report, you certify that you have read and agree to abide by the guidelines stated in this policy for conducting security research and disclosure of vulnerabilities or indicators of vulnerabilities related to the CVLE system. If you submit such a report, we will presume you are acting in good faith when you discover, test, and submit reports of vulnerabilities[3] or indicators of vulnerabilities in accordance with the guidelines stated herein, which include the following:

- You MAY[4] test the CVLE system to detect a vulnerability or identify an indicator related to a vulnerability for the sole purpose of providing the CVLE staff with information about such vulnerability.
- You MUST avoid harm to the CVLE system and operations.
- You MUST NOT exploit any vulnerability beyond the minimal amount of testing required to prove that the vulnerability exists or to identify an indicator related to that vulnerability.
- You MUST NOT intentionally access the content of any communications, data, or information transiting or stored on the CVLE system except to the extent that the information is directly related to a vulnerability and the access is necessary to prove that the vulnerability exists.
- You MUST NOT exfiltrate any data under any circumstances.
- You MUST NOT intentionally compromise the privacy or safety of the Edgesource personnel, CVLE staff, or CVLE audience members.
- You MUST NOT intentionally compromise the intellectual property or other commercial or financial interests of Edgesource personnel or entities or any legitimate third parties.
- You MUST NOT disclose any details of any extant CVLE system vulnerability or indicator of vulnerability to any party not already aware at the time the report is submitted to Edgesource.
- In the event that you find a vulnerability in the CVLE consequent to a vulnerability in a generally available product, you MAY report the product vulnerability to the affected vendor or a third-party vulnerability coordination service in order to enable the product to be fixed.
- You MAY disclose to the public the prior existence of vulnerabilities already fixed by the CVLE staff, potentially including details of the vulnerability, indicators of vulnerability, or the nature (but not content) of information rendered available by the vulnerability. If you choose to disclose, you must first receive advance written permission from Edgesource.
- You MUST NOT disclose any incidental proprietary data revealed during testing or the content of information rendered available by the vulnerability to any party not already aware at the time the report is submitted to Edgesource.
- You MUST NOT disclose any confidential information, any Personal Identifying Information (PII), or any other protected information.
- You MUST NOT cause a denial of any legitimate services in the course of your testing.
- You MUST NOT conduct social engineering in any form of Edgesource personnel or subcontractors.
- You SHOULD strive to submit high-quality reports.
- You MUST NOT submit a high-volume of low-quality reports.

- You MUST comply with all applicable Federal, State, and local laws in connection with security research activities or other participation in this vulnerability disclosure program.

If at any point you are uncertain of whether to proceed with testing, please contact our team at VDP@edgesource.net.

6.0 PARTICIPANT EXPECTATIONS

We take every disclosure seriously, and very much appreciate your efforts. We are committed to coordinating with you as openly and expeditiously as possible. The contents of information provided in the reports and follow-up communications are processed and stored on an Edgesource information system. You can expect us to do the following:

- We WILL investigate every reported vulnerability and strive to ensure that appropriate steps are taken to mitigate risk and remediate reported vulnerabilities.
- If you opt to provide your contact information, our security team MAY contact you for further information.
- We SHALL, to the best of our ability, validate the existence of the vulnerability.
- We MAY disclose to the public the prior existence of vulnerabilities remedied by us, potentially including details of the vulnerability such as the indicators of vulnerability, or the nature (but not content) of information rendered available by the vulnerability.
- In the event that we choose to publicly disclose your reported vulnerability we SHALL recognize your contribution as it must pertain to improving our security, the first to report a unique vulnerability, and if your report triggers a code or configuration change.
- In the event you report a vulnerability pertaining to a generally available product, we SHALL validate the vulnerability pertaining to the identified product is legitimate and that it is a product used within our environment. After those factors are verified, we MAY report the product vulnerability to the affected vendor or to a third-party vulnerability coordination service.
- We SHALL NOT forward your name and contact information to any affected vendors unless otherwise requested by you.
- We MAY NOT disclose information provided by any vendor unless the vendor explicitly states to do so.
- We SHALL request 30 days for acknowledgement and 90 days for mitigation development, and deployment.
- We MAY consult with you and any affected vendors to determine our public disclosure5 plans of the vulnerability
- In cases where a product is affected and the vendor is unresponsive, or fails to establish a reasonable timeframe for remediation, we MAY disclose product vulnerabilities 45 days after

the initial contact is made, regardless of the existence or availability of patches or workarounds from affected vendors.

7.0 LEGAL / AUTHORIZATION

If you make a good faith effort to conduct your research and disclose vulnerabilities in accordance with the guidelines set forth in this policy, and if your activities within the VDP to identify vulnerabilities otherwise do not break any laws, Edgesource will not recommend or pursue any law enforcement or civil lawsuits related to such activities. This agreement is effective at the time of the form submission to Edgesource.

Please note that individuals and entities that conduct activities as authorized by this policy and comply with its terms MAY receive legal protection from criminal or civil liability under section 1030 of title 18, United States Code, and similar laws penalizing unauthorized access to computers.

Edgesource does not authorize, permit, or otherwise allow (expressly or implicitly) any person, including any individual, group of individuals, consortium, partnership, or any other business or legal entity to engage in any security research or vulnerability or threat disclosure activity that is inconsistent with this policy or the law. Any activities that are inconsistent with this policy or the law may lead to criminal and/or civil liabilities. Third parties (e.g., any non-Edgesource entity) may independently determine whether to pursue legal recourse or related.

Edgesource may modify the terms of this policy or suspend this policy at any time.

---

[1] These websites constitute "information systems" as defined by 44 U.S.C. 3502.
[2] The term "Researcher" in this document is intended to be consistent with the terms "Finder" and/or "Reporter" as used in ISO/IEC 29147:2014(E) and the CERT Guide to Coordinated Vulnerability Disclosure, and may be substituted with "you, your".
[3] Vulnerabilities throughout this policy may be considered "security vulnerabilities" as defined by Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 102. The term "security vulnerability" means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.
[4] The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.
[5] "Public disclosure" means the release of previously undisclosed information related to a vulnerability by Edgesource, another vendor, or a researcher to [the public/non-governmental persons or entities] through mediums that include, but are not limited to, official press releases, blogs, social media platforms, email, or other webpages. We SHALL make our disclosure determinations based on relevant factors, such as: whether the vulnerability has already been publicly disclosed, the severity of the vulnerability, potential impact to critical infrastructure, possible threat to public health and safety, immediate mitigations available, vendor responsiveness and feasibility for creating an upgrade or patch, and vendor estimate of time required for customers to obtain, test, and apply the patch. Active exploitation, threats of an especially serious nature, or situations that require changes to an established standard may result in earlier or later disclosure.

Edgesource/CVLE Vulnerability Disclosure Program (VDP) Policy And Rules Of Engagement (ROE)

Version 1.0, June 30, 2023