Vulnerability Disclosure Policy

June 1, 2021

Introduction

National Council on Disability (NCD) is committed to ensuring the security of the American public by protecting their information. This policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our preferences in how to submit discovered vulnerabilities to NCD. We expect potential vulnerabilities in our systems to be reported immediately so we can initiate an action to mitigate the vulnerability.

This policy describes:

- What systems and types of research are covered under this policy;
- How to send us vulnerability reports; and,
- How long we ask security researchers to wait before publicly disclosing vulnerabilities.

Authorization

If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized and we will work with you to understand and resolve the issue quickly, and NCD will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.

Guidelines

Under this policy, “research” means activities in which you:

- Notify us as soon as possible after you discover a real or potential security issue;

- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data;
- Only use exploits to the extent necessary to confirm a vulnerability's presence;
- Do not use an exploit to compromise or exfiltrate data, establish persistent command line access, or use the exploit to pivot to other systems;
- Provide us a reasonable amount of time no more than 90 days to resolve the issue before you disclose it publicly; and
- Do not submit a high volume of low-quality reports.

Once you have established that a vulnerability exists or encounter any sensitive data, including personally identifiable information, financial information, or proprietary information or trade secrets of any party, you must stop your test, notify us immediately, and not disclose this data to anyone else.

Test Methods

The following test methods are not authorized:

- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data; and,
- Physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing.

Scope

This policy applies to the following systems and services:

- NCD.GOV
- NCD systems or services

Any service not expressly listed above, such as any connected services, are excluded from scope and are not authorized for testing. Additionally, vulnerabilities found in systems from our vendors fall outside of the scope of this policy and should be reported directly to the vendor according to their disclosure policy. If the vendor does not have a disclosure policy, vulnerabilities will be reported to the primary point of contact (POC)

and all other parties listed in the contract or agreement, including the Contracting Officer (CO), if applicable. If you are not sure whether a system is in scope or not, contact us at security@agency.gov before starting your research or at the security contact for the system's domain name listed in Whois - DOTGOV.

Though we develop and maintain other internet-accessible systems or services, we ask that active research and testing only be conducted on the systems and services covered by the scope of this document. If there is a particular system not in scope that is identified for testing, you must obtain authorization to conduct any additional testing not previously authorized. NCD retains the authority to change the scope of this policy at any time deemed necessary and in response to federal requirements and directives.

Reporting a Vulnerability

NCD will make every reasonable attempt to establish email communication with the vendor's security team, up to a maximum of three attempts. If we are unable to identify an official email for the security team, we will initiate contact with the primary POC and all other parties listed in the contract or agreement, including the CO, if applicable. NCD will provide the vendor with information about the discovered vulnerabilities, a link to this policy, a tracking identifier, and a notification that the planned disclosure date is 90 days from when the vulnerabilities were disclosed to the vendor or other reporting authority.

NCD is committed to the following notification schedule:

- The initial attempt when the vulnerability is identified;
- A second attempt no less than one week after the initial attempt; and
- A third attempt no less than two weeks after the initial attempt.

If a response is not received from the vendor within 45 days of the initial attempt, NCD will notify CERT/CC, ICS-CERT, or a national CERT. NCD will notify CERT if no response is received, and after 45 days of notification CERT will publicly publish as required.

Working Together

NCD has a vested interest in our vendors and our policy is to be responsive, professional and provide assistance when vulnerabilities are identified. NCD will work with vendors with the goal of keeping all systems and data safe and all vendors will work with NCD to address vulnerabilities and keep the agency informed of actions taken by the vendor to mitigate identified vulnerabilities.

The following updates are expected on a regular basis and no less than 48 hours from the initial vulnerability update and no more than 15 days following any action. This includes notifications and updates on:

- When the vulnerability was confirmed;
- When it was passed to the development team;
- When a patch(es) is planned to be released as well as when they are released, the patch encompasses software fixes for vulnerabilities as well as other forms of remediation or mitigation provided by the vendor; and,
- All other pertinent information relating to the efforts of the vendor in addressing the reported vulnerability.

NCD recognizes that external messaging may be important to the vendor. If desired, our outreach team will work with the vendor to develop joint press releases and synchronize on messaging within the timelines established in this policy.

Information submitted under this policy will be used for defensive purposes only, to mitigate or remediate vulnerabilities. If your findings include newly discovered vulnerabilities that affect all users of a product or service and not solely NCD, we may share your report with the Cybersecurity and Infrastructure Security Agency, where it will be handled under their coordinated vulnerability disclosure process. We will not share your name or contact information without express permission.

We accept vulnerability reports at security@agency.gov. Reports may be submitted anonymously. If you share contact information, we will acknowledge receipt of your report within 3 business days.

We do not support PGP-encrypted emails. For particularly sensitive information, submit through our website at https://ncd.gov/about.

Vendor Responsibilities

To help us triage and prioritize submissions, vendor reports must:

- Describe the location the vulnerability was discovered and the potential impact of exploitation;
- Offer a detailed description of the steps needed to reproduce the vulnerabilities., proof of concept scripts and screenshots, if available; and
- Communication in English, if possible.

NCD Responsibilities

When you choose to share your contact information with us, we commit to coordinating with you as openly and as quickly as possible.

- Within 3 business days, we will acknowledge that your report has been received;
- To the best of our ability, we will confirm the existence of the vulnerability to you and be as transparent as possible about what steps we are taking during the remediation process, including issues or challenges that may delay resolution; and,
- We will maintain an open dialogue to discuss issues.

This policy will continue to be in effect even if the vendor has prior knowledge of the vulnerability disclosed by NCD.

Document Change History

Version	Date	Description
1.0	06/01/2021	First issuance.