Vulnerability Disclosure Policy

Introduction

CONA Services LLC (CONA) is committed to ensuring the security of our solutions and data. This Policy is intended to give security researchers clear guidelines for conducting vulnerability discovery activities and to convey our requirements on how to submit discovered vulnerabilities to us. This Policy describes what systems and types of research are covered under this Policy, how to send us vulnerability reports, and what you can expect from us.

We encourage you to contact us to report potential vulnerabilities in our systems. See below under "Reporting a Vulnerability" on how to contact us.

Authorization

If you comply fully 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. If you have complied with this Policy, CONA does not intend to recommend or pursue legal action related to your research.

Please review and ensure that you agree with all terms of this Policy before conducting any research of CONA internet-accessible systems or services, and before submitting a report. By submitting a report, we consider you to have agreed to compliance with this Policy.

Guidelines

Under this policy, "research" means activities in which you, in good faith, seek out potential security vulnerabilities in any digital asset owned, operated, or maintained by CONA, or a circumstance that could reasonably impact the security of our Company or our users, and we encourage you disclose this to us. In doing so, we require that you:

- Stop testing and notify us immediately 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 efforts or exploits to the extent necessary to confirm a vulnerability's presence. Do not do anything to compromise or exfiltrate data, establish persistent command line access, or make efforts to pivot to other systems.
- Provide us with a reasonable amount of time to resolve any issue.
- Do not submit a high volume of low-quality reports.

Once you've 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**. Depending on the nature of the data, we may also ask that you properly dispose of any data you obtained or otherwise might exist on any devices from which you performed research.

Scope

The sole areas in which we authorize you to conduct research are in our non-production environment, including such systems marked as “development” or “test”. You are prohibited from conducting research related to our operational production environment, and we reserve all our legal rights if you do so.

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 this Policy’s scope and should be reported directly to the vendor according to their disclosure policy (if any). If you aren’t sure whether a system is in scope or not, contact us at **security at conaservices dot com** before starting your research.

Though we develop and maintain other internet-accessible systems or services, active research and testing may only be conducted on the systems and services covered by the scope of this document.

For greater certainty, the following activities are explicitly out of scope of this policy.

- Failing to immediately delete/destroy sensitive information or personal data you may inadvertently access.
- Publicly disclosing any potential vulnerability without the express written consent of CONA.
- Intentionally or negligently causing a denial-of-service condition for any user beyond the researcher.
- Exploitation of any vulnerability which sends bulk unsolicited or unauthorized messages (spam).
- Conducting research through social engineering or other deceptive means.
- Conducting research by physically connecting to a network or device within a facility operated by CONA or any of its vendors or partners.

Test methods

The following test methods are not authorized:

- Testing any system other than the systems set forth in the 'Scope' section above.
- Network denial of service (DoS or DDoS) tests or other tests that impair access to or damage a system or data.
- Physical testing (e.g., office access, open doors, tailgating), social engineering (e.g., phishing, vishing), or any other non-technical vulnerability testing.
- Introducing malicious software.
- Deleting, altering, sharing, retaining, or destroying CONA data, or rendering the data inaccessible.

Reporting a vulnerability

CONA will accept vulnerability reports via this form, please provide all known information related to the suspected security vulnerability you are reporting. If you choose to share contact information, we will acknowledge receipt of your report within 3 business days.

By submitting a vulnerability, you acknowledge that you have no expectation of payment and that you expressly waive any future pay claims against CONA Services LLC related to your submission.

What we expect from you

- We request that you communicate information about potential security vulnerabilities in a responsible manner. This means complying with all applicable laws and the respecting the privacy of individuals. Your security research should also avoid degradation of our user's experiences, disruption to systems, and destruction of data.
- We request that researchers provide sufficient technical detail and background necessary for our team to identify and validate reported issues, using the link below.
- We request that researchers act for the common good, protecting user privacy and security by refraining from publicly disclosing vulnerabilities.

Reports should provide a detailed technical description of the steps required to reproduce the vulnerability, including a description of any tools needed to identify or exploit the vulnerability. Images, e.g., screen captures, and other documents may be attached to reports. It is helpful to give attachments illustrative names. Reports may include proof-of-concept code or screenshots that demonstrate exploitation of the vulnerability.

What you can expect from us

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

- 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 on issues or challenges that may delay resolution.
- We will maintain an open dialogue to discuss issues, and we will maintain standard confidentiality in our communications with you.
- We will investigate and use all reasonable efforts to remediate validated issues in a manner consistent with protecting the safety and security of those potentially affected by a reported vulnerability.
- We reserve all of CONA's legal rights in the event of noncompliance with this Policy, but it does not intend to pursue legal action against any party that conducts security research and discloses information to us in good faith and as outlined in this Policy.

Classified: General Business