Censis Technologies, Inc.
4031 Aspen Grove Drive
Suite 350
franklin, TN 37067

615-468-8000
888-877-3010 toll-free
615-468-8003 fax
www.censis.com

Vulnerability Disclosure Policy

Introduction

Censis is committed to ensuring the integrity of its information by securing its information systems. A vulnerability is a "weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source." This Vulnerability Disclosure Policy (VDP) is meant to address some of the possible apprehensions and explain what research would be authorized under this VDP. Good faith research that conforms to these guidelines is considered authorized research. Censis will focus on quickly working to resolve the vulnerability you have identified and is not interested in pursuing legal action when there is authorized research under this policy.

This policy describes what systems and types of research are covered under this policy, how to report the vulnerability, how long Censis asks security researchers to wait before publicly disclosing vulnerabilities and what communication or response to expect from us.

Authorization

Censis welcomes the chance to hear from good faith security researchers, who conduct security research under these VDP guidelines. This VDP is meant to address some of the possible apprehensions and explain that working within this VDP is the best way to ensure the research will be authorized. Good faith research is not considered a security breach if it follows the guidelines below. Once Censis sees it is authorized research, we want to focus on quickly working to resolve the vulnerability you have identified and is not interested in pursuing legal action. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, Censis will make this authorization known.

Requirements

These guidelines require that the researcher:

- Access Censis systems in a way that follows this VDP.
- If you discover a vulnerability, report it by following the instructions in this VDP.
- Make every effort to avoid privacy violations, degradation of user experience, disruption to production systems, and destruction or manipulation of data.
- Limit the use of discovered exploits to the extent necessary to confirm a vulnerability's presence.
- Do not use an exploit to compromise or exfiltrate data, establish command line access and/or persistence, or use the exploit to pivot to other systems.
- Provide Censis with a reasonable amount of time to resolve the issue before you disclose it publicly.
- Do not submit a high volume of low-quality vulnerability reports.

If you established that a vulnerability or security weakness exists or encounter any sensitive data or data belonging to individuals with their financial information, medical information, contract information, or proprietary information which might be a trade secret, **you must stop your test, notify Censis immediately, and not disclose this data to anyone else.**

Test Methods

The following test methods are **not** authorized or considered good faith/authorized research:

- 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, smishing), or any other non-technical vulnerability testing.

Scope

This policy applies to the following systems and services:

```
*.censis.com
*.censis.net
*.loanerlink.com
*.appliedlogicinc.com
*.impress-connect.com
*.wearemaestro.com
*.mysurgicaltracking.com
```

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 Censis 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 Censis using the Reporting process in the section below before starting your research.

Though Censis develops and maintains 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 system not in scope that you think merits testing, please contact Censis using the report process below to discuss it first.

Reporting a Vulnerability

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 for Censis, we may share your report with the Cybersecurity and Infrastructure Security Agency (CISA), where it will be handled under their coordinated vulnerability disclosure process. Censis will not share your name or contact information without express permission. Censis will acknowledge receipt of your report within 3 business days. Censis will not offer payment or compensation for good faith research.

Go to the https://censis.com/contact-us/ website to submit a vulnerability report.

Complete all the required fields in the form and select '**Vulnerability Reporting**' in the reason for inquiry menu. Click the submit button to send your vulnerability report.

Expectations

What Censis would like to see from you

In order to help us triage and prioritize submissions, we recommend that your reports:

- Describe the location the vulnerability was discovered and the potential impact of exploitation.
- Offer a detailed description of the steps needed to reproduce the vulnerability (proof of concept scripts are helpful).
- Be in English.

Censis Technologies, Inc.
4031 Aspen Grove Drive
Suite 350
franklin, TN 37067

615-468-8000
888-877-3010 toll-free
615-468-8003 fax
www.censis.com

What you can expect from Censis

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.
- We will maintain an open dialogue to discuss issues.

Questions

Questions regarding this policy may be submitted using the same contact-us form to report vulnerabilities. We also invite you to contact us with suggestions for improving this policy.

For broader questions, refer to the CISA Vulnerability Disclosure Process at https://www.cisa.gov/coordinated-vulnerability-disclosure-process