TEKTELIC Communications Inc.
7657 10th Street NE Calgary, Alberta
Canada, T2E 8X2

TEKTELIC Vulnerability Disclosure Policy

Introduction

TEKTELIC is a global leader in developing LPWAN IoT end-to-end solutions. TEKTELIC's IoT product portfolio includes sensors, gateways, servers and application software.

This vulnerability disclosure policy applies to any vulnerabilities related to TEKTELIC products. Please read this vulnerability disclosure policy fully to ensure you act in compliance before reporting a vulnerability.

We value those who take the time and effort to report security vulnerabilities according to this policy. However, we do not offer financial compensation for vulnerability disclosures.

Reporting procedures

If you believe you have found a security vulnerability, please submit your report to us in English via a ticket in our support portal (https://support.tektelic.com). Please use the ticket category “Potential Vulnerability“ and please include details of the following:

- The product and version on which the vulnerability can be observed. For web-based applications, please provide the website, IP or page where the vulnerability can be observed.
- A brief description of the type of vulnerability, for example “Privilege escalation vulnerability”.
- Steps to reproduce or a benign, non-destructive, proof of concept.

This helps to ensure that the report can be triaged quickly and accurately. It also reduces the likelihood of duplicate reports.

What to expect

After you have submitted your report, we will respond to your report within 5 working days and triage your report within 10 working days. We’ll also aim to keep you informed of our progress.

Priority for remediation is assessed by looking at the impact, severity and exploit complexity. Vulnerability reports might take some time to triage or address. You are

welcome to inquire on the status but should avoid doing so more than once every 14 days. This allows our teams to focus on the remediation.

We will notify you when the reported vulnerability is remediated, and you may be invited to confirm that the fix adequately addresses the vulnerability. During this time, we ask that you refrain from publicly disclosing the vulnerability until we have had a chance to alert our customers and distribute the fix.

Guidelines

TEKTELIC does not endorse or encourage the following behavior:

- Breaking any applicable laws or regulations.
- Accessing, modifying or disrupting any of TEKTELIC's systems, services or data.
- Social engineering, phishing or physically attacking TEKTELIC's staff or infrastructure.
- Submitting reports that use high-intensity invasive or destructive scanning tools to find vulnerabilities.
- Reporting any form of denial of service, e.g. overwhelming a service with a high volume of requests.
- Communicating any vulnerabilities or associated details other than by means described in the published security.txt.
- Disclosing any data retrieved from TEKTELIC's systems or services in the course of your research.
- Keeping any data obtained in the course of your research longer than absolutely necessary under data protection regulations.

Disclaimer

This policy is designed to be compatible with common vulnerability disclosure good practice. It does not give you permission to act in any manner that is inconsistent with the law, or which might cause TEKTELIC or partner organizations to be in breach of any legal obligations.