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

Software Update and Patching Policy

Introduction

TEKTELIC is responsible for providing timely updates to vulnerable software. The goal of this policy is to outline TEKTELIC's procedures with regards to updating software in the presence of security vulnerabilities.

End of life notification

TEKTELIC will announce any changes to the support status of our devices here: https://support.tektelic.com/portal/en/community/tektelic-announcements/announcements. Expiry of support for a device will be provided at least 90 days in advance.

Monitoring for vulnerabilities

For supported products, TEKTELIC will routinely monitor avenues for known security issues and updates. Monitoring includes but is not limited to:

- Reviewing security mailing lists.
- Reviewing vendor notifications.
- Review submissions from our vulnerability disclosure program: https://support.tektelic.com/portal/en/kb/articles/submitting-vulnerability-reports.
- Scanning released software for known vulnerabilities from the National Vulnerability Database.

Auditing reports

Once alerted to a potential vulnerability in a supported product, TEKTELIC will review any reports or patches to see if a vulnerability exists and classify it if necessary, according to one of the following categories:

- **Critical**: If TEKTELIC determines that we are vulnerable and this issue can be actively exploited.
- **Non-critical**: If TEKTELIC determines that we may be vulnerable, but it is not deemed a high-risk, exploitable issue.

- **Not applicable**: If TEKTELIC determines we are not considered vulnerable. We will not plan to address these issues.

TEKTELIC will look at metrics such as CVSS score, local configuration and acceptable business risk when classifying vulnerabilities.

Verification of fixes

TEKTELIC will apply any updates as required and verify the fix with our testing team. When we are satisfied that the update(s) adequately address the vulnerability, we will schedule a release.

- For critical vulnerabilities, we will provide a hotfix to address the issue. This will be released immediately.
- For non-critical vulnerabilities, we will include the fix in the next planned software release.

User responsibilities

New software releases are communicated through TEKTELIC's support portal available here: https://support.tektelic.com/portal/en/community/tektelic-announcements/announcements. Customers should regularly monitor this for new releases.

Customers are responsible for performing software updates for the following products:

- KONA Gateway products, updates can be performed using any of the following tools:
  - KONA Core Network Server
  - KONA Element OA&M Server
  - KONA Pilot Field Tool
  - Command-line access
- KONA Core Network Server, if the server is locally hosted updates are coordinated with TEKTELIC staff.

The following products have their updates applied automatically:

- TEKTELIC Device/Sensor products. These are always updated to the latest software during manufacturing.
- KONA Network servers that are cloud hosted updates are applied periodically by TEKTELIC staff.
- Other cloud-hosted servers and applications have their updates automatically applied by TEKTELIC staff.