Cybersecurity of Verbatim Gen2 and RMC

For the RACO Verbatim Gen2 and RACO Monitoring Center

The Verbatim Gen2 RTU communicates outbound-only over encrypted cellular connections. Devices do not accept inbound connections and have no publicly routable IP address. All data in transit uses TLS 1.2+. User access is managed through Auth0 with MFA support

1. **Network Security:**
    1. We have implemented firewalls and network segmentation to secure our network infrastructure and prevent unauthorized access.
    2. We filter and control outbound DNS traffic for our VPCs using a reputable cloud service.
    3. All services are firewalled from the internet and only allow HTTP/s traffic.
    4. All pages shall be encrypted using TLS 1.2 with SHA256 hash algorithm and a 2048-bit key, utilizing certificates from a major Certificate Authority (CA).
    5. RACO shall not sell any information collected through its web application.
    6. RACO shall not display advertisements of any kind within customer company web areas.
2. **Software Security:**
    1. Our software application has been updated with the latest security patches, and our development process includes security testing to identify and fix potential vulnerabilities before they can be exploited.
    2. The RACO Monitoring Center operates on a **serverless, cloud-native infrastructure** orchestrated using Kubernetes.
    3. The platform follows an **ongoing weekly patching process**, powered by automated dependency monitoring tools (e.g., Dependabot) to identify and remediate known vulnerabilities in third-party libraries and components.
    4. Infrastructure and services are **self-updating** and automatically redeploy in response to:

Phone: (800) 722-6999
Website: racoman.com
727 Allston Way, Berkeley, CA 94710

1. Security updates
2. Platform updates
3. Scalability events (e.g., increased load)
4. Infrastructure events (e.g., server outages)

5. RACO maintains **automated unit test coverage and a CI/CD pipeline** that validates changes prior to deployment.
6. Application updates are **rolled out incrementally with zero downtime**, and are deployed to production only when automated tests pass, reducing the risk of regression or service interruption.

3. **Data Encryption:**
    1. Sensitive data transmitted between our devices and the cloud is encrypted to protect against eavesdropping and unauthorized access.
    2. TLS certificates are provisioned and managed with cloud services and connected resources.
    3. User passwords are not stored in our system. We use a third-party authentication service (Auth0) to securely manage user credentials. This service supports single sign-on (SSO) and federated authentication via OIDC to providers including Google, Microsoft, and others.
    4. RTU traffic flows into our cloud infrastructure over an encrypted connection to our telemetry provider.
4. **Access Control:**
    1. Access to our systems and data is strictly controlled through the use of unique login credentials and multi-factor authentication.
    2. API access control is managed using OIDC and short-lived JWT bearer tokens, preventing XSS attacks on cookies.
    3. Servers and managed services receive security patches on an ongoing basis.
    4. Granular user controls segregate access between administrators and users on the RACO Monitoring Center website. Only relevant information is shown to users who are granted access and permission.
    5. Customers are encouraged to enable multi-factor authentication for user accounts.

Phone: (800) 722-6999
Website: racoman.com
727 Allston Way, Berkeley, CA 94710

6. Users may optionally establish individual user PINs for alarm acknowledgment and call-in access.

5. **Continuous Monitoring:**
    1. Our system is monitored 24/7 for any signs of unauthorized access or security breaches
    2. Incident response procedures are in place to identify, investigate, and remediate security incidents in a timely manner.
6. **Device Operating System Security:**
    1. The Verbatim Gen2 runs a minimal, hardened Debian Linux image with only the packages and services required for device operation.
    2. The device has no general internet access – all communication is confined to a narrow cellular telemetry channel, limiting the attack surface to that single pathway.
    3. RACO monitors Debian security advisories for packages included in the device image on an ongoing basis.
    4. Critical OS patches are triaged by severity: only vulnerabilities affecting components that are installed and running on the device trigger action.
    5. Patches requiring a system-level OS update are applied on-site via USB-C connection using the RMC app or SD card swap at the device. No specialized technical knowledge is required.
    6. Between updates, the device continues to operate normally with no degradation in functionality or security posture.

We take the security of our customers' data very seriously, and we are constantly working to improve our cybersecurity measures to ensure that we remain at the forefront of the industry. If you have any questions or concerns, please don't hesitate to reach out to our team.

Phone: (800) 722-6999
Website: racoman.com
727 Allston Way, Berkeley, CA 94710

This documentation is provided for informational purposes only and is subject to change without notice. Verbatim Gen2 is not a life-safety system. These materials do not modify or replace the RACO Terms of Service.

RACO Manufacturing & Engineering
727 Allston Way, Suite B
Berkeley, CA 94710

Toll free: +1-800-722-6999
sales@racoman.com
www.racoman.com/verbatim