SOLIDWARETOOLS

CRACheck

DOCUMENT 3

Cybersecurity Risk Assessment

Art. 13.2-4 + Annex I

NovaBridge Technologies Inc.

NovaBridge SmartHub v3.1

Reference: CRACHK-Y8IV87
Date of issuance: 15/10/2026
Contact: Sarah Chen, VP of Compliance
compliance@novabridge.io

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 (Cyber Resilience Act)

This document does not constitute legal advice. Sole responsibility of the manufacturer.

>> ASSESSMENT CONTEXT

This risk assessment documents the analysis performed pursuant to Art. 13.2 of Regulation (EU) 2024/2847, taking into account the intended purpose, the reasonably foreseeable use and the conditions of use of the product, with the aim of minimising cybersecurity risks, preventing incidents and minimising their impact.

PRODUCT ASSESSED

NovaBridge SmartHub v3.1

INTENDED PURPOSE

WiFi/Zigbee smart home hub for centralised control of smart home devices (lights, smart locks, security cameras, motion and temperature sensors). Includes iOS/Android mobile app and cloud backend (AWS eu-west-1) for remote access and push notifications. Intended for residential consumers in the EU, sold through Amazon.de, Amazon.fr and Amazon.es.

OPERATING ENVIRONMENT

Residential homes in the EU. The hub is connected to the home WiFi router and to the manufacturer cloud (AWS eu-west-1) for remote access; Zigbee devices pair locally. Installed and used by non-expert consumers. Reasonably foreseeable misuse: default network left unsecured, product exposed to the internet through port forwarding by the user.

ASSESSED SUPPORT PERIOD

5 years

This document does not constitute legal advice. Sole responsibility of the manufacturer.

>> ESSENTIAL REQUIREMENTS — PART I: PRODUCT PROPERTIES (Annex I)

For each requirement of Annex I, Part I, it is indicated whether it applies to the product and the implementation is described or, if not applicable, the justification pursuant to Art. 13.4.

(a) No known exploitable vulnerabilities

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(a)]

Full CVE scan of all dependencies (Snyk) and penetration test (NCC Group, report NCG-2026-0412) completed on 15/03/2026. 0 critical or high vulnerabilities pending at launch time. Pre-release verification process documented in the QMS.

(b) Secure by default configuration

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(b)]

Factory configuration: WiFi disabled until initial setup, unique admin credentials per device (factory-generated with CSPRNG), Zigbee pairing mode disabled by default. Factory reset available: physical button (5 seconds) + app option + local web interface option.

(c) Security updates

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(c)]

Automatic OTA updates enabled by default. The user can disable them from Settings > System > Automatic updates. Push notification when an update is available. Security updates separated from functional ones when technically feasible. Option to postpone update for up to 7 days.

(d) Protection against unauthorised access

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(d)]

Email/password authentication + optional MFA (TOTP). JWT sessions, 24h expiry. Access control: admin / standard user / guest. Logging of all access attempts (successful and failed) with IP, timestamp and user-agent. Account lockout after 5 failed attempts (30 min).

(e) Data confidentiality

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(e)]

TLS 1.3 for all hub-cloud and app-cloud communication. AES-256-GCM for sensitive data at rest (WiFi credentials, tokens). X.509 certificates with pinning in the mobile app. Zigbee with AES-128-CCM encryption (Zigbee 3.0 standard).

(f) Data integrity

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(f)]

This document does not constitute legal advice. Sole responsibility of the manufacturer.

Secure boot with Ed25519 firmware signature verification on every boot. Configuration integrity verification via HMAC-SHA256. Digital signature of all OTA update packages. Automatic report to user if unauthorised configuration modification is detected.

(g) Data minimisation

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(g)]

Data collected: device configuration, programmed scenes, event logs (last 30 days), cloud authentication token. No home usage data, audio/video recordings (cameras are processed locally), or precise geolocation is collected. Retention policy: logs automatically deleted after 30 days.

(h) Availability and resilience

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(h)]

Offline mode: the hub works as a local Zigbee controller without internet connection. Rate limiting on the cloud API: 100 req/min per user. Automatic recovery after power cut (persistent state in flash). Watchdog timer for automatic restart in case of firmware hang.

(i) Minimise impact on other devices

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(i)]

Network isolation: the hub does not act as a router or forward traffic between Zigbee devices and the internet. Outbound traffic control limited to NovaBridge cloud endpoints (domain whitelist). No UPnP, no automatic port opening.

(j) Minimise attack surface

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(j)]

Only 3 open ports: 443 (HTTPS for local web interface), 8883 (MQTT over TLS for cloud communication), Zigbee port (radio, not IP). SSH and Telnet services disabled in production. Debug interface disabled in production firmware. Principle of least privilege: each firmware process runs with the minimum necessary permissions.

(k) Incident impact mitigation

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(k)]

Firmware processes isolated via Linux namespaces. Read-only firmware partition (squashfs). User data on separate partition. Automatic rollback to previous firmware if the update fails post-installation integrity verification. Compartmentalisation: compromise of one service does not compromise the entire system.

(l) Security logging and monitoring

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(l)]

Security logs: access events, configuration changes, firmware updates, Zigbee events (pairing/unpairing), failed access attempts. Stored locally (last 30 days) and optionally synced to cloud (encrypted). The user can disable cloud sync from Settings > Privacy. Local logs cannot be disabled (needed for diagnostics).

(m) Secure data erasure

APPLIES

IMPLEMENTATION [Annex I, Part I, 2(m)]

Full factory reset: physical button (5 sec) or from the app (Settings > System > Restore factory defaults). Erases: WiFi credentials, cloud tokens, configurations, scenes, logs, paired Zigbee devices. Data export: the user can download their data in JSON format from the app before resetting. The transfer is done over HTTPS.

This document does not constitute legal advice. Sole responsibility of the manufacturer.

>> THREAT AND RISK REGISTER (Art. 13.2-13.3)

For each requirement of Annex I, Part I, the threat it addresses, the risk rated by the manufacturer before the measures described above and the residual risk after them.

REQ.	THREAT ADDRESSED	RISK BEFORE	MEASURES	RESIDUAL RISK
(a)	Exploitation of known vulnerabilities in the product or its components	High	See (a) above	Medium
(b)	Compromise through insecure default settings or default credentials	High	See (b) above	Low
(c)	Vulnerabilities left open because updates are missing or fail	High	See (c) above	Low
(d)	Unauthorised access to the product, its functions or its data	High	See (d) above	Low
(e)	Disclosure of data stored, transmitted or processed	High	See (e) above	Low
(f)	Manipulation of data, commands, programs or configuration	High	See (f) above	Low
(g)	Processing more data than needed, increasing exposure	Medium	See (g) above	Low
(h)	Loss of essential functions, including denial-of-service	Medium	See (h) above	Medium
(i)	Use of the product to harm other devices or networks	Medium	See (i) above	Low
(j)	Exploitation of unnecessary interfaces or services	High	See (j) above	Low
(k)	An incident spreading or escalating its impact	Medium	See (k) above	Low
(l)	Malicious activity going undetected	Medium	See (l) above	Low
(m)	Data remaining on the product after decommissioning	Medium	See (m) above	Low

Residual risks rated High: 0. Any residual risk rated High should be reviewed before the product is placed on the market. Requirements left unrated must be rated by the manufacturer.

This document does not constitute legal advice. Sole responsibility of the manufacturer.

>> ESSENTIAL REQUIREMENTS — PART II: VULNERABILITY MANAGEMENT (Annex I)

(1) Vulnerability identification and documentation + SBOM

SBOM [Part II, point 1]

Yes — SBOM generated and maintained — CycloneDX

(2) Vulnerability remediation

PROCESS [Part II, point 2]

Classification by CVSS v3.1. Critical (CVSS ≥9.0): patch within 24-48h, immediate user notification. High (CVSS 7.0-8.9): patch within 7 days. Medium (CVSS 4.0-6.9): patch within 30 days. Low (CVSS <4.0): included in the next scheduled release. All security updates are free of charge during the support period. Information about fixed vulnerabilities published at https://www.novabridge.io/security/advisories after patch availability (Annex I, Part II, point 4).

(3) Regular tests and reviews

PROCESS [Part II, point 3]

Quarterly penetration testing by NCC Group (latest report: NCG-2026-0412, March 2026). Static code analysis with SonarQube on every commit (0 blocker/critical allowed for merge). Weekly dependency vulnerability scanning with Snyk (integrated into CI/CD). Zigbee and MQTT protocol fuzzing with AFL++ before every major release. Manual security code review by the security team before every release.

(4) Disclosure of fixed vulnerabilities

PROCESS [Part II, point 4]

Information published on the manufacturer's website after patch availability. Includes description, affected products, impact, severity and remediation measures.

(5) Coordinated Vulnerability Disclosure (CVD) policy

CVD POLICY [Part II, point 5]

Coordinated disclosure policy published at https://www.novabridge.io/security/cvd-policy. Reporting channel: security@novabridge.io + HTTPS web form. Commitment to acknowledgement within 48 business hours. Target remediation time: 90 days from vulnerability confirmation. Coordinated public disclosure after patch availability. Active bug bounty programme on HackerOne (https://hackerone.com/novabridge) with $100-$5,000 rewards based on CVSS severity.

(6) Vulnerability contact point

CONTACT [Part II, point 6]

security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (EST hours)

(7) Secure update distribution

MECHANISM [Part II, point 7]

OTA (Over-The-Air) with Ed25519 digital package signing. TLS 1.3 end-to-end encrypted channel. Firmware integrity verification (SHA-256) before and after installation. Automatic rollback to previous firmware in case of verification failure. Security updates separated from functional ones whenever technically feasible. Each security update remains available for download for a minimum of 10 years (Art. 13.9).

(8) Free security updates

POLICY [Part II, point 8]

All security updates are provided free of charge during the support period (5 years). Each update remains available for download for a minimum of 10 years pursuant to Art. 13.9.

This document has been generated by CRACheck (SolidwareTools) from the information provided by the manufacturer. It does not constitute legal advice or a third-party audit. The accuracy of the data and effective compliance with applicable legal obligations are the sole responsibility of the manufacturer. The structure follows Regulation (EU) 2024/2847 as reviewed by SolidwareTools at the date of issuance. For personalised advice, consult a qualified professional.