

VULNERABILITY DISCLOSURE POLICY

Versione 1.0

Data di emissione: 11/09/2026

Proprietario del documento: ELCA S.r.l.

Contatto: cybersecurity@elcaradio.com

1. Scopo

La presente Vulnerability Disclosure Policy definisce le modalità attraverso cui ELCA riceve, valuta e gestisce le segnalazioni di vulnerabilità di sicurezza relative ai propri prodotti e servizi.

ELCA riconosce l'importanza della collaborazione con clienti, partner, ricercatori di sicurezza e utilizzatori finali al fine di migliorare continuamente il livello di sicurezza dei propri prodotti e ridurre i potenziali rischi associati a vulnerabilità informatiche.

La presente policy è stata definita in coerenza con i principi del Cyber Resilience Act (Regolamento UE 2024/2847) e con le pratiche internazionali di Coordinated Vulnerability Disclosure.

2. Ambito

La presente policy si applica alle vulnerabilità che riguardano:

- prodotti ELCA con componenti digitali;
- firmware installato nei prodotti ELCA;
- applicazioni software sviluppate e distribuite da ELCA;
- strumenti di configurazione e diagnostica eventualmente forniti da ELCA;
- servizi digitali direttamente gestiti da ELCA e connessi ai propri prodotti.

Non rientrano nell'ambito della presente policy:

- richieste di assistenza tecnica;
- reclami commerciali;
- richieste di garanzia;
- problematiche non correlate alla sicurezza informatica.

Per tali richieste rimangono validi i normali canali di assistenza ELCA.

3. Come effettuare una segnalazione

Le vulnerabilità possono essere segnalate inviando una comunicazione all'indirizzo: cybersecurity@elcaradio.com

La segnalazione dovrebbe contenere, per quanto possibile:

- nome e recapito del segnalante;
 - prodotto interessato;
 - versione del firmware o del software interessato;
 - descrizione della vulnerabilità;
 - modalità con cui la vulnerabilità è stata individuata;
 - passaggi necessari per riprodurre il problema;
 - livello di impatto osservato;
 - eventuali log, foto, video o documentazione tecnica di supporto.
- La completezza delle informazioni facilita l'analisi e la gestione della segnalazione.

4. Gestione delle segnalazioni

Ogni segnalazione ricevuta viene registrata e sottoposta ad una valutazione preliminare da parte del personale tecnico incaricato. ELCA si impegna a:

- confermare la ricezione della segnalazione entro un tempo ragionevole;
- valutare la validità tecnica delle informazioni ricevute;
- classificare il rischio associato alla vulnerabilità;
- definire le eventuali azioni correttive necessarie;

VULNERABILITY DISCLOSURE POLICY

Version 1.0

Issue Date: 11/09/2026

Document Owner: ELCA S.r.l.

Contact: cybersecurity@elcaradio.com

1. Purpose

This Vulnerability Disclosure Policy defines the procedures through which ELCA receives, assesses and manages reports of security vulnerabilities affecting its products and services.

ELCA recognises the importance of collaboration with customers, partners, security researchers and end users in order to continuously improve the security of its products and reduce the potential risks associated with cybersecurity vulnerabilities.

This policy has been established in accordance with the principles of the Cyber Resilience Act (EU Regulation 2024/2847) and international Coordinated Vulnerability Disclosure practices.

2. Scope

This policy applies to vulnerabilities affecting:

- ELCA products with digital components;
- Firmware installed in ELCA products;
- Software applications developed and distributed by ELCA;
- Configuration and diagnostic tools provided by ELCA, where applicable;
- Digital services directly managed by ELCA and connected to its products.

This policy does not apply to:

- Technical support requests;
- Commercial complaints;
- Warranty claims;
- Issues not related to cybersecurity.

For such requests, ELCA's standard support channels remain applicable.

3. How to Submit a Vulnerability Report

Vulnerabilities may be reported by sending a communication to: cybersecurity@elcaradio.com

Where possible, the report should include:

- Name and contact details of the reporter;
- Product concerned;
- Affected firmware or software version;
- Description of the vulnerability;
- Method by which the vulnerability was identified;
- Steps required to reproduce the issue;
- Observed level of impact;
- Any supporting logs, photographs, videos or technical documentation.

Providing complete information helps facilitate the assessment and management of the report.

4. Handling of Reports

Each report received is logged and subject to a preliminary assessment by the designated technical personnel.

ELCA undertakes to:

- Acknowledge receipt of the report within a reasonable time;
- Assess the technical validity of the information provided;
- Classify the risk associated with the vulnerability;
- Define any necessary corrective actions;



• mantenere, ove possibile, un dialogo con il segnalante durante il processo di gestione.

L'adozione di una specifica misura correttiva rimane in ogni caso subordinata alle verifiche tecniche, alla valutazione del rischio e alla fattibilità dell'intervento.

5. Coordinated Vulnerability Disclosure

ELCA promuove un approccio di divulgazione responsabile e coordinata delle vulnerabilità.

Si invita pertanto il segnalante a:

- comunicare la vulnerabilità esclusivamente a ELCA prima di renderla pubblica;
- concedere a ELCA un periodo ragionevole per l'analisi e la correzione del problema;
- collaborare con ELCA qualora siano necessari chiarimenti tecnici.

A sua volta ELCA si impegna a valutare le segnalazioni ricevute in modo imparziale e ad adottare le misure ritenute necessarie per la tutela dei propri clienti e utilizzatori.

6. Attività consentite

ELCA incoraggia le attività di ricerca svolte in buona fede e finalizzate esclusivamente all'identificazione responsabile di vulnerabilità.

Il segnalante deve:

- operare nel rispetto delle leggi applicabili;
- evitare interruzioni dei servizi;
- evitare alterazioni dei dati;
- limitare le attività al minimo necessario per dimostrare l'esistenza della vulnerabilità;
- interrompere immediatamente le attività qualora venga rilevato l'accesso accidentale a dati di terzi.

7. Attività non consentite

Non sono consentite attività che possano:

- compromettere la disponibilità dei prodotti o dei servizi;
- causare danni a ELCA, ai suoi clienti o a terzi;
- comportare accessi non autorizzati a dati personali o informazioni riservate;
- prevedere la diffusione pubblica di dettagli tecnici della vulnerabilità prima del completamento delle attività di analisi e gestione;
- comportare l'installazione di malware o software dannoso.

8. Comunicazioni e divulgazione pubblica

Qualora una vulnerabilità venga confermata e corretta, ELCA potrà pubblicare comunicazioni tecniche, note di rilascio o altri avvisi informativi ritenuti opportuni.

Salvo diverso accordo tra le parti, ELCA potrà riconoscere il contributo del segnalante nelle forme ritenute appropriate.

9. Trattamento dei dati personali

I dati personali eventualmente trasmessi nell'ambito della segnalazione saranno trattati da ELCA esclusivamente per le finalità connesse alla gestione della vulnerabilità e nel rispetto della normativa applicabile in materia di protezione dei dati personali.

Per ulteriori informazioni si rimanda all'Informativa Privacy disponibile sul sito www.elcaradio.com.

10. Limitazioni

La presente policy non conferisce alcun diritto di compenso economico per le segnalazioni effettuate.

ELCA non gestisce programmi di bug bounty e non prevede

• Maintain, where possible, communication with the reporter throughout the handling process.

The adoption of any specific corrective measure remains subject to technical verification, risk assessment and implementation feasibility.

5. Coordinated Vulnerability Disclosure

ELCA promotes a responsible and coordinated approach to vulnerability disclosure.

Reporters are therefore requested to:

- Disclose the vulnerability exclusively to ELCA before making it public;
- Allow ELCA a reasonable period of time to analyse and remediate the issue;
- Cooperate with ELCA where technical clarification is required.

In turn, ELCA undertakes to assess all reports impartially and to adopt the measures deemed necessary to protect its customers and users.

6. Permitted Activities

ELCA encourages security research activities carried out in good faith and solely for the responsible identification of vulnerabilities.

The reporter must:

- Act in compliance with applicable laws;
- Avoid disruption of services;
- Avoid alteration of data;
- Limit activities to the minimum necessary to demonstrate the existence of the vulnerability;
- Immediately cease activities if accidental access to third-party data is discovered.

7. Prohibited Activities

Activities that may:

- Compromise the availability of products or services;
 - Cause damage to ELCA, its customers or third parties;
 - Involve unauthorised access to personal data or confidential information;
 - Include the public disclosure of technical details relating to a vulnerability before the analysis and management process has been completed;
 - Involve the installation of malware or other malicious software.
- are not permitted.

8. Communications and Public Disclosure

Where a vulnerability is confirmed and remediated, ELCA may publish technical communications, release notes or other informational notices considered appropriate.

Unless otherwise agreed between the parties, ELCA may acknowledge the reporter's contribution in a manner deemed appropriate.

9. Personal Data Processing

Any personal data submitted as part of a vulnerability report will be processed by ELCA solely for purposes related to the management of the vulnerability and in accordance with applicable data protection legislation.

For further information, please refer to the Privacy Notice available at www.elcaradio.com.

10. Limitations

This policy does not confer any right to financial compensation for reported vulnerabilities.

ELCA does not operate a bug bounty programme and does not provide monetary rewards or financial incentives for the



premi o riconoscimenti economici per la scoperta di vulnerabilità.

11. Aggiornamenti della policy

ELCA si riserva il diritto di modificare la presente policy in qualsiasi momento per adeguarla all'evoluzione normativa, tecnologica e organizzativa.

La versione aggiornata sarà sempre disponibile sul sito web aziendale.

discovery of vulnerabilities.

11. Policy Updates

ELCA reserves the right to amend this policy at any time in order to reflect legal, technological or organisational developments.

The latest version will always be available on the company website.

