POLITICA DI DIVULGAZIONE COORDINATA DELLE VULNERABILITÀ

1. Scopo

Lo scopo della presente politica di divulgazione coordinata delle vulnerabilità è descrivere le modalità mediante le quali AUTEC riceve, gestisce e divulga le vulnerabilità dei prodotti con elementi digitali di cui AUTEC è fabbricante.

2. Applicabilità

Quanto descritto nella presente politica di divulgazione coordinata delle vulnerabilità si applica ai prodotti con elementi digitali, che AUTEC mette a disposizione del mercato, rientranti nel campo di applicazione del regolamento (UE) 2024/2847[1].

La presente politica di divulgazione coordinata delle vulnerabilità è applicabile a partire dal 11 settembre 2026.

3. Definizioni

Prodotto con elementi digitali: qualsiasi prodotto software o hardware e le relative soluzioni di elaborazione dati da remoto, compresi i componenti software o hardware, immesso sul mercato separatamente; nel seguito del presente documento per brevità si utilizzerà il termine “prodotto”.

Periodo di assistenza: il periodo durante il quale un fabbricante garantisce che le vulnerabilità di un prodotto con elementi digitali siano gestite in modo efficace e conformemente ai requisiti essenziali di cibersicurezza.

Vulnerabilità: un punto debole, una suscettibilità o un difetto di prodotti TIC[2] o servizi TIC che può essere sfruttato da una minaccia informatica.

Vulnerabilità sfruttabile: una vulnerabilità che può essere utilizzata efficacemente da un avversario in condizioni operative pratiche.

Vulnerabilità attivamente sfruttata: una vulnerabilità per la quale esistono prove attendibili che un soggetto malintenzionato l’ha sfruttata in un sistema senza l’autorizzazione del proprietario del sistema.

Incidente: un evento che compromette la disponibilità, l’autenticità, l’integrità o la riservatezza di dati conservati, trasmessi o elaborati o dei servizi offerti dai sistemi informatici e di rete o accessibili attraverso di essi[3].

Incidente grave: un incidente che ha un impatto sulla sicurezza del prodotto con elementi digitali è considerato grave se[4]:

- incide negativamente o è in grado di incidere negativamente sulla capacità di un prodotto con elementi digitali di proteggere la disponibilità, l’autenticità, l’integrità o la riservatezza di dati o funzioni sensibili o importanti;

oppure

- ha portato o è in grado di portare all’introduzione o all’esecuzione di un codice maligno in un prodotto con elementi digitali o nei sistemi informativi e di rete di un utilizzatore del prodotto con elementi digitali.

4. Principi generali

AUTEC riconosce il valore della collaborazione con la comunità dei ricercatori sulla sicurezza informatica e con gli utilizzatori dei prodotti di cui AUTEC è fabbricante e si impegna a:

- promuovere la segnalazione responsabile delle vulnerabilità;

COORDINATED VULNERABILITY DISCLOSURE POLICY

1. Purpose

The purpose of this Coordinated Vulnerability Disclosure Policy is to describe how AUTEC receives, manages and discloses vulnerabilities in products with digital elements that AUTEC manufactures.

2. Applicability

The provisions of this Coordinated Vulnerability Disclosure Policy apply to products with digital elements, which AUTEC makes available to the market, falling within the scope of Regulation (EU) 2024/2847[1].

This Coordinated Vulnerability Disclosure Policy is applicable as of September 11, 2026.

3. Definitions

Product with digital elements: Any software or hardware product and related remote data processing solutions, including software or hardware components, placed on the market separately; the term “product” shall be used later in this document for brevity.

Support period: the period during which a manufacturer ensures that vulnerabilities in a product with digital elements are managed effectively and in accordance with the essential cybersecurity requirements.

Vulnerability: A weakness, susceptibility or defect in ICT products[2] or ICT services that can be exploited by a cyber threat.

Exploitable vulnerability: A vulnerability that can be effectively used by an adversary under practical operating conditions.

Actively exploited vulnerability: A vulnerability for which there is strong evidence that an attacker exploited it on a system without the system owner’s permission.

Incident: an event that compromises the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed or of the services offered by or accessible through computer and network systems[3].

Severe Incident: An incident having an impact on the security of products with digital elements is considered severe if[4]:

- adversely affects or is likely to adversely affect the ability of a digitally manufactured product to protect the availability, authenticity, integrity or confidentiality of sensitive or important data or functions;

or

- has led or is likely to lead to the introduction or execution of malicious code in a product with digital elements or in the information and network systems of a user of the product with digital elements

4. General principles

AUTEC recognizes the value of collaboration with the cybersecurity research community and users of the products AUTEC manufactures and is committed to:

- promote responsible reporting of vulnerabilities;

- garantire la riservatezza delle informazioni ricevute;
- trattare le segnalazioni con diligenza, tempestività e imparzialità;
- coordinare la divulgazione pubblica delle vulnerabilità, ove appropriato;
- astenersi dall'intraprendere azioni legali nei confronti dei soggetti che segnalano vulnerabilità che operino in conformità alla presente politica di divulgazione coordinata delle vulnerabilità e alle disposizioni legislative vigenti.

5. Segnalazione delle vulnerabilità

5.1. Modalità di segnalazione delle vulnerabilità

AUTEC ha istituito i seguenti punti di contatto mediante i quali chiunque può segnalare le vulnerabilità emerse sui prodotti:

- indirizzo di posta elettronica cybersecurity@autecsafety.com
- modulo presente nella pagina https://www.autecsafety.com/it/cybersecurity del sito internet aziendale.

La ricezione della segnalazione è confermata al soggetto che ha segnalato la vulnerabilità tramite posta elettronica.

5.2. Contenuto della segnalazione delle vulnerabilità

La segnalazione della vulnerabilità deve contenere almeno le seguenti informazioni:

- indirizzo di posta elettronica a cui può essere contattato il soggetto che segnala la vulnerabilità;
- identificativo del prodotto su cui è stata riscontrata la vulnerabilità, compreso numero seriale, codice impianto e/o model e type del prodotto;
- descrizione della vulnerabilità rilevata, delle condizioni in cui si manifesta e se si sospetta che sia il risultato di atti illegittimi o malevoli;
- ogni altra informazione utile a contestualizzare le condizioni in cui la vulnerabilità si manifesta.

6. Analisi e correzione delle vulnerabilità

Le vulnerabilità che sono state segnalate ai punti di contatto indicati nel paragrafo 5.1 vengono tempestivamente analizzate da AUTEC. Dall'analisi può emergere che:

- la vulnerabilità riguarda un prodotto per il quale il periodo di assistenza è terminato:

1. in questo caso AUTEC dà riscontro al soggetto che ha segnalato la vulnerabilità spiegando che il periodo di assistenza del prodotto è terminato;

- la vulnerabilità riguarda un prodotto per il quale il periodo di assistenza è in corso:

2. e la vulnerabilità riguarda un componente integrato nel prodotto; in questo caso AUTEC dà riscontro al soggetto che ha segnalato la vulnerabilità specificando che la segnalazione della vulnerabilità è stata inoltrata al fabbricante del componente interessato e indicando ogni eventuale altra azione intrapresa per attenuare l'impatto della vulnerabilità;
3. e non sono necessari aggiornamenti software o modifiche del prodotto; in questo caso, AUTEC dà riscontro al soggetto che ha segnalato la vulnerabilità spiegando perché non può compromettere la sicurezza informatica del prodotto;

- guarantee the confidentiality of the information received;
- deal with reports with diligence, timeliness and impartiality;
- coordinate the public disclosure of vulnerabilities, where appropriate;
- refrain from taking legal action against individuals reporting vulnerabilities that operate in accordance with this Coordinated Vulnerability Disclosure Policy and applicable law.

5. Vulnerability reporting

5.1. How vulnerabilities are reported

AUTEC has established the following points of contact through which anyone can report vulnerabilities that have emerged on products:

- cybersecurity@autecsafety.com e-mail address;
- form on the page https://www.autecsafety.com/cybersecurity of the company website.

Receipt of the report is confirmed to the person who reported the vulnerability by e-mail.

5.2. Vulnerability reporting content

The vulnerability report must contain at least the following information:

- the e-mail address at which the person reporting the vulnerability can be contacted;
- identifier of the product on which the vulnerability was found, including serial number, plant code and/or product model and type;
- a description of the vulnerability detected, the conditions under which it manifests itself and whether it is suspected to be the result of illegitimate or malicious acts;
- any other information useful for contextualizing the conditions in which the vulnerability occurs.

6. Vulnerability analysis and remediation

Vulnerabilities that have been reported to the points of contact listed in paragraph 5.1 are promptly analyzed by AUTEC. The analysis may show that:

- The vulnerability affects a product for which the support period has ended:

1. in this case, AUTEC acknowledges the person who reported the vulnerability by explaining that the product's support period has ended;

- The vulnerability affects a product for which the support period is ongoing:

2. and the vulnerability concerns a component integrated into the product; in this case, AUTEC acknowledges the person who reported the vulnerability by specifying that the vulnerability report has been forwarded to the manufacturer of the affected component and indicating any other action taken to mitigate the impact of the vulnerability;
3. and no software updates or product modifications are required; in this case, AUTEC responds to the person who reported the vulnerability by explaining why it cannot compromise the IT security of the product;

4. ed è necessario effettuare una campagna di richiamo dei prodotti interessati dalla vulnerabilità per apportare le necessarie modifiche;

5. e sono necessari aggiornamenti software del prodotto; in questo caso gli aggiornamenti vengono gestiti secondo le modalità descritte nel paragrafo 6.1.

6.1. Aggiornamenti software di sicurezza dei prodotti

Sulla base delle analisi effettuate secondo le modalità descritte nel paragrafo 6, AUTEC:

- predispone gli aggiornamenti software di sicurezza necessari;
- individua i prodotti e le versioni interessate dagli aggiornamenti;
- identifica i clienti originari dei prodotti coinvolti;
- comunica tempestivamente a tali soggetti, tramite posta elettronica o altri canali appropriati, le istruzioni per l'applicazione degli aggiornamenti.

Qualora l'aggiornamento non sia applicabile da remoto o dall'utilizzatore, AUTEC provvede a de-finire modalità alternative di intervento, inclusi, ove necessario, richiami del prodotto per aggiornamento del software.

Gli aggiornamenti software rimangono disponibili dopo il rilascio per un minimo di 10 anni o per il restante periodo di assistenza, se quest'ultimo è superiore.

7. Divulgazione delle informazioni sulle vulnerabilità

Una volta reso disponibile un aggiornamento software di sicurezza AUTEC prepara un documento contenente le seguenti informazioni:

- codice identificativo univoco della segnalazione di vulnerabilità;
- tipo e modello del prodotto interessato dalle vulnerabilità ed eventualmente altre informazioni utili per identificarlo in modo univoco (ad esempio versione);
- descrizione, gravità e impatto delle vulnerabilità;
- indicazioni su come correggere le vulnerabilità (ad esempio, installazione di aggiornamenti software, configurazione del prodotto, modalità di richiamo dei prodotti, ecc.).

Tali informazioni sono comunicate immediatamente:

- mediante posta elettronica al soggetto che ha segnalato la vulnerabilità.
- mediante posta elettronica agli utilizzatori noti dei prodotti interessati dalle vulnerabilità.

Informazioni di sintesi potrebbero essere divulgate pubblicandole sul sito internet aziendale.

8. Condotte ammesse e non ammesse

8.1. Condotte ammesse

È consentito svolgere attività di test di sicurezza sul sistema oggetto di analisi esclusivamente nella misura strettamente necessaria a dimostrare l'esistenza della vulnerabilità, evitando qualsiasi impatto sui sistemi, sui dati e sugli utenti.

8.2. Condotte non ammesse

È fatto divieto di:

- accedere, modificare o estrarre dal sistema oggetto di analisi

4. and a recall campaign of the affected products must be carried out to make the necessary changes;

5. and product software updates are required; in this case, updates are managed according to the methods described in paragraph 6.1.

6.1. Product Security Software Updates

On the basis of the analyses carried out in accordance with the procedures described in paragraph 6, AUTEC:

- prepares the necessary security software updates;
- identify the products and versions affected by the updates;
- identifies the original customers of the products involved;
- promptly communicate to such parties, by e-mail or other appropriate channels, instructions for applying updates.

If the update is not applicable remotely or by the user, AUTEC will define alternative methods of intervention, including, where necessary, product recalls for software updates.

Software updates remain available after release for a minimum of 10 years or for the remainder of the support period, whichever is longer.

7. Vulnerability Information Disclosure

Once a security software update is made available, AUTEC prepares a document containing the following information:

- unique identification code of the vulnerability report;
- type and model of the product affected by the vulnerabilities and possibly other information useful for uniquely identifying it (e.g. version);
- description, severity and impact of vulnerabilities;
- guidance on how to fix vulnerabilities (e.g., installing software updates, configuring the product, how to recall products, etc.).

This information shall be communicated immediately:

- by e-mail to the person who reported the vulnerability.
- by e-mail to known users of the affected products.

Summary information may be disclosed by publishing it on the company website.

8. Permitted and prohibited conduct

8.1. Permitted conduct

Security testing activities on the system under investigation may only be carried out to the extent strictly necessary to demonstrate the existence of the vulnerability, avoiding any impact on systems, data and users.

8.2. Prohibited conduct

It is forbidden to:

- access, modify, or extract personal, confidential, or sensitive

dati personali, riservati o sensibili non necessari alla segnalazione della vulnerabilità;

- compromettere la disponibilità dei servizi del sistema oggetto di analisi (ad esempio mediante attacchi di negazione del servizio);
- introdurre malware nel sistema oggetto di analisi;
- copiare, modificare o eliminare dati nel sistema oggetto di analisi;
- apportare modifiche al sistema oggetto di analisi;
- accedere ripetutamente al sistema oggetto di analisi o condividere l'accesso al sistema oggetto di analisi con altri;
- eseguire attacchi brute force per ottenere l'accesso a un sistema;
- sfruttare la vulnerabilità per finalità diverse dalla segnalazione;
- divulgare pubblicamente la vulnerabilità senza preventiva autorizzazione scritta di AUTEC.

9. Riconoscimento dei soggetti che segnalano le vulnerabilità

AUTEC si riserva la facoltà, a propria esclusiva discrezione, di riconoscere i contributi forniti dai soggetti che abbiano segnalato vulnerabilità in modo valido e conforme alla presente Politica di Divulgazione Coordinata delle Vulnerabilità. Tali riconoscimenti possono includere:

- la pubblicazione del nominativo dell'interessato in appositi elenchi di ringraziamento, previo suo consenso;
- a citazione dell'interessato nei documenti di divulgazione delle vulnerabilità di cui al paragrafo 7, previo suo consenso;

10. Aggiornamenti della politica di divulgazione coordinata delle vulnerabilità

La presente politica di divulgazione coordinata delle vulnerabilità potrà essere modificata o aggiornata in qualsiasi momento. La versione vigente è resa disponibile alla pagina https://www.autecsafety.com/it/cybersecurity del sito internet aziendale ed è vincolante a partire dalla data di applicazione indicata nella politica di divulgazione coordinata delle vulnerabilità.

[1] Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio del 23 ottobre 2024 relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciber-resilienza).

[2] TIC: tecnologie dell'informazione e della comunicazione.

[3] Direttiva (UE) 2022/2555, articolo 6, punto 6).

[4] Regolamento (UE) 2024/2847, articolo 14.

data from the system under analysis that is not necessary for reporting the vulnerability;

- compromise the availability of the services of the system under investigation (e.g. through denial-of-service attacks);
- introduce malware into the system being analyzed;
- copy, modify, or delete data in the system being analyzed;
- make changes to the system being analyzed;
- repeatedly access the system being scanned or sharing access to the system being scanned with others;
- perform brute force attacks to gain access to a system;
- exploit the vulnerability for purposes other than reporting;
- publicly disclose the vulnerability without prior written permission from AUTEC.

9. Recognition of Vulnerability Reporting Entities

AUTEC reserves the right, in its sole discretion, to recognize contributions made by individuals who have reported vulnerabilities in a valid manner and in accordance with this Coordinated Vulnerability Disclosure Policy. Such awards may include:

- the publication of the name of the interested party in special thank-you lists, subject to his/her consent;
- the reference of the data subject in the vulnerability disclosure documents referred to in paragraph 7, subject to the data subject's consent;

10. Updates to the coordinated vulnerability disclosure policy

This Coordinated Vulnerability Disclosure Policy may be modified or updated at any time. The current version is made available on the page https://www.autecsafety.com/cybersecurity of the company website and is binding from the date of application indicated in the coordinated vulnerability disclosure policy.

[1] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act).

[2] ICT: Information and communication technologies.

[3] Directive (EU) 2022/2555, Article 6(6).

[4] Regulation (EU) 2024/2847, Article 14.