



Single Reporting Platform di ENISA

Scheda

Certifico Srl - IT

ID 27230 | 05 Ottobre 2026

La piattaforma è il canale unico e obbligatorio attraverso cui le aziende segnalano vulnerabilità e incidenti di sicurezza, garantendo una rete di allarme rapido su scala europea, raggiungibile all'indirizzo portal.cra-srp.enisa.europa.eu.

L'obiettivo principale della piattaforma è semplificare gli adempimenti normativi previsti dall'Articolo 14 del CRA. In passato, la gestione di una vulnerabilità o di un attacco grave richiedeva la notifica separata alle diverse autorità nazionali.

Con l'entrata in funzione della SRP, i produttori di hardware e software (e in prospettiva anche i gestori di software open-source) possono inviare un'unica segnalazione centralizzata. Il sistema provvede poi a smistare automaticamente la notifica sia al CSIRT (Computer Security Incident Response Team) nazionale coordinatore di competenza, sia ai sistemi centrali dell'ENISA.

Le segnalazioni riguardano principalmente due categorie di eventi:

- **Vulnerabilità attivamente sfruttate** (Actively exploited vulnerabilities): falle di sicurezza per le quali si registrano attacchi concreti in corso nel mondo reale.

- **Incidenti gravi di sicurezza** (Severe incidents): eventi tali da compromettere significativamente la riservatezza, l'integrità o la disponibilità del prodotto o dei dati associati.

Per garantire un intervento tempestivo a tutela degli utenti e dell'intero mercato unico, la piattaforma impone scadenze di notifica estremamente stringenti.

Tre fasi:

Avviso tempestivo (Early Warning) - **Entro 24 ore**: Non appena viene rilevata una vulnerabilità sfruttata o un incidente grave, il produttore deve inviare una prima segnalazione essenziale entro un solo giorno.

Notifica dettagliata - **Entro 72 ore**: A tre giorni dalla prima segnalazione, è necessario integrare la pratica con una valutazione iniziale del rischio e le contromisure attuate o raccomandate agli utenti.

Relazione finale (Final Report):

Per le vulnerabilità: il report conclusivo va trasmesso **entro 14 giorni** dal rilascio della patch o dell'aggiornamento correttivo.

Per gli incidenti gravi: la relazione va chiusa **entro 1 mese** dalla notifica dettagliata.

L'accesso alla Single Reporting Platform è severamente regolamentato. Per procedere con le comunicazioni obbligatorie, i rappresentanti aziendali (Assigned Representative) devono autenticarsi tramite il sistema EU Login dotato di autenticazione a due fattori (MFA).

Attualmente, l'uso operativo del portale è riservato ai soli produttori soggetti agli obblighi di legge o ai loro rappresentanti ufficiali. Le segnalazioni ordinarie da parte di ricercatori indipendenti, distributori o utenti continuano invece a seguire i canali tradizionali dei CSIRT territoriali o i programmi di vulnerability disclosure delle singole aziende.

Guardando ai prossimi sviluppi, l'ENISA prevede di estendere le funzionalità del portale introducendo un modulo per la segnalazione volontaria, che permetterà a qualsiasi persona fisica o giuridica di condividere minacce e vulnerabilità, rafforzando la cyber-resilienza complessiva dello spazio europeo.

Regolamento (UE) 2024/2847 / Cyber Resilience Act

Articolo 14 Obblighi di segnalazione dei fabbricanti

1. Un fabbricante notifica simultaneamente al CSIRT designato come coordinatore, conformemente al paragrafo 7 del presente articolo, e all'ENISA, qualsiasi vulnerabilità attivamente sfruttata contenuta nel prodotto con elementi digitali di cui viene a conoscenza. Il fabbricante notifica tale vulnerabilità attivamente sfruttata tramite la piattaforma unica di segnalazione istituita a norma dell'articolo 16.

2. Ai fini della notifica di cui al paragrafo 1, il fabbricante presenta:

- a) una notifica di preallarme di una vulnerabilità attivamente sfruttata, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui il fabbricante ne è venuto a conoscenza, che indichi, se del caso, gli Stati membri sul cui territorio il fabbricante sia al corrente del fatto che il suo prodotto con elementi digitali è stato messo a disposizione;
- b) a meno che non siano già state fornite le informazioni pertinenti, una notifica delle vulnerabilità, senza indebito ritardo e in ogni caso entro 72 ore dal momento in cui il fabbricante è venuto a conoscenza della vulnerabilità attivamente sfruttata, che fornisca informazioni generali, se disponibili, sul prodotto con elementi digitali interessato, sulla natura generale dello sfruttamento e della vulnerabilità in questione, nonché sulle eventuali misure correttive o di attenuazione adottate e sulle misure correttive o di attenuazione che gli utilizzatori possono adottare, e che indichi anche, se del caso, il grado di sensibilità attribuito dal fabbricante alle informazioni notificate;
- c) a meno che non siano già state fornite le informazioni pertinenti, una relazione finale, entro 14 giorni dalla messa a disposizione di una misura correttiva o di attenuazione, che comprenda almeno:
 - i) una descrizione della vulnerabilità, compresi la sua gravità e il suo impatto;
 - ii) se disponibili, informazioni relative a qualsiasi soggetto malintenzionato che abbia sfruttato o che sfrutti la vulnerabilità;
 - iii) informazioni dettagliate relative all'aggiornamento di sicurezza o ad altre misure correttive messe a disposizione per porre rimedio alla vulnerabilità.

3. Un fabbricante notifica simultaneamente al CSIRT designato come coordinatore, conformemente al paragrafo 7 del presente articolo, e all'ENISA, qualsiasi incidente grave che abbia un impatto sulla sicurezza del prodotto con elementi digitali di cui viene a conoscenza. Il fabbricante notifica tale incidente tramite la piattaforma unica di segnalazione istituita a norma dell'articolo 16.

4. Ai fini della notifica di cui al paragrafo 3, il fabbricante presenta:

- a) una notifica di preallarme di un incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali, senza indebito ritardo e in ogni caso entro 24 ore dal momento in cui il fabbricante ne è venuto a conoscenza, che precisi, come minimo, se si sospetta che l'incidente sia il risultato di atti illegittimi o malevoli, e che indichi, se del caso, gli Stati membri sul cui territorio il fabbricante sia al corrente del fatto che il suo prodotto con elementi digitali è stato messo a disposizione;
- b) a meno che non siano già state fornite le informazioni pertinenti, una notifica dell'incidente, senza indebito ritardo e in ogni caso entro 72 ore dal momento in cui il fabbricante ne è venuto a conoscenza, che fornisca informazioni generali, se disponibili, sulla natura dell'incidente, una valutazione iniziale dell'incidente, nonché le eventuali misure correttive o di attenuazione adottate e le misure correttive o di attenuazione che gli utilizzatori possono adottare, e che indichi anche, se del caso, il grado di sensibilità attribuito dal fabbricante alle informazioni notificate;
- c) a meno che non siano già state fornite le informazioni pertinenti, una relazione finale entro un mese dalla trasmissione della notifica di incidente di cui alla lettera b), che comprenda almeno:
 - i) una descrizione dettagliata dell'incidente, comprensiva della sua gravità e del suo impatto;
 - ii) il tipo di minaccia o la causa di fondo che ha probabilmente innescato l'incidente;
 - iii) le misure di attenuazione adottate e in corso;

5. Ai fini del paragrafo 3, un incidente che ha un impatto sulla sicurezza del prodotto con elementi digitali è considerato grave se:

- a) 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; o

b) 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.

6. Se necessario, il CSIRT designato come coordinatore che ha ricevuto per primo la notifica può chiedere ai fabbricanti di fornire una relazione intermedia sui pertinenti aggiornamenti della situazione sulla vulnerabilità attivamente sfruttata o sull'incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali.

7. Le notifiche di cui ai paragrafi 1 e 3 del presente articolo sono trasmesse attraverso la piattaforma unica di segnalazione di cui all'articolo 16 utilizzando uno dei terminali per la notifica elettronica di cui all'articolo 16, paragrafo 1. La notifica è trasmessa utilizzando il terminale per la notifica elettronica del CSIRT designato come coordinatore dello Stato membro in cui i fabbricanti hanno lo stabilimento principale nell'Unione ed è contemporaneamente accessibile all'ENISA.

Ai fini del presente regolamento, si considera che un fabbricante abbia il suo stabilimento principale nell'Unione nello Stato membro in cui sono prevalentemente adottate le decisioni relative alla cibersicurezza dei suoi prodotti con elementi digitali. Se non è possibile determinare detto Stato membro, si considera che lo stabilimento principale sia nello Stato membro in cui il fabbricante ha lo stabilimento con il maggior numero di dipendenti nell'Unione.

Se non ha uno stabilimento principale nell'Unione, il fabbricante trasmette le notifiche di cui ai paragrafi 1 e 3 utilizzando il terminale per la notifica elettronica del CSIRT designato come coordinatore nello Stato membro determinato secondo l'ordine seguente e sulla base delle informazioni a disposizione del fabbricante:

- a) lo Stato membro in cui è stabilito il rappresentante autorizzato che agisce per conto del fabbricante per il maggior numero di prodotti con elementi digitali di tale fabbricante;
- b) lo Stato membro in cui è stabilito l'importatore che immette sul mercato il maggior numero di prodotti con elementi digitali di tale fabbricante;
- c) lo Stato membro in cui è stabilito il distributore che mette a disposizione sul mercato il maggior numero di prodotti con elementi digitali di tale fabbricante;
- d) lo Stato membro in cui è situato il maggior numero di utilizzatori di prodotti con elementi digitali di tale fabbricante.

In relazione al terzo comma, lettera d), un fabbricante può presentare notifiche relative a qualsiasi successiva vulnerabilità attivamente sfruttata o incidente grave che ha un impatto sulla sicurezza del prodotto con elementi digitali allo stesso CSIRT designato come coordinatore a cui ha presentato la prima notifica.

8. Dal momento in cui è venuto a conoscenza di una vulnerabilità attivamente sfruttata o di un incidente grave avente un impatto sulla sicurezza del prodotto con elementi digitali, il fabbricante informa gli utilizzatori interessati del prodotto con elementi digitali e, se del caso, tutti gli utilizzatori, di tale vulnerabilità o incidente e, se necessario, di qualsiasi attenuazione dei rischi e misure correttive che gli utilizzatori possono adottare per attenuare l'impatto di tale vulnerabilità o incidente, se del caso in un formato strutturato, leggibile da un dispositivo automatico e che possa essere facilmente elaborato automaticamente. Se il fabbricante non informa tempestivamente gli utilizzatori del prodotto con elementi digitali, i CSIRT designati come coordinatori che hanno ricevuto la notifica possono fornire tali informazioni agli utilizzatori se ritenuto proporzionato e necessario per prevenire o attenuare l'impatto di tale vulnerabilità o incidente.

9. Entro l'11 dicembre 2025 la Commissione adotta atti delegati conformemente all'articolo 61 per integrare il presente regolamento specificando i termini e le condizioni per l'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione delle notifiche di cui all'articolo 16, paragrafo 2. La Commissione coopera con la rete di CSIRT istituita a norma dell'articolo 15 della direttiva (UE) 2022/2555 e con l'ENISA nella preparazione dei progetti di atti delegati.

10. La Commissione può, mediante atti di esecuzione, specificare ulteriormente il formato e le procedure di trasmissione delle notifiche di cui al presente articolo, nonché agli articoli 15 e 16. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 62, paragrafo 2. La Commissione coopera con la rete di CSIRT e con l'ENISA nella preparazione del progetto di atto delegato.

[...]

Articolo 16 Istituzione di una piattaforma unica di segnalazione

1. Ai fini delle notifiche di cui all'articolo 14, paragrafi 1 e 3, e all'articolo 15, paragrafi 1 e 2, e per semplificare gli obblighi di segnalazione dei fabbricanti, l'ENISA istituisce una piattaforma unica di segnalazione. Le operazioni quotidiane di tale piattaforma unica di segnalazione sono gestite e mantenute dall'ENISA. L'architettura della piattaforma unica di segnalazione consente agli Stati membri e all'ENISA di predisporre i propri terminali per la notifica elettronica.

2. Dopo aver ricevuto una notifica, il CSIRT designato come coordinatore che ha ricevuto per primo la notifica la diffonde senza ritardo attraverso la piattaforma unica di segnalazione ai CSIRT designati come coordinatori sul cui territorio il fabbricante ha indicato che il prodotto con elementi digitali è stato messo a disposizione.

In circostanze eccezionali e, in particolare, su richiesta del fabbricante e alla luce del grado di sensibilità delle informazioni notificate indicato dal fabbricante a norma dell'articolo 14, paragrafo 2, lettera a), del presente regolamento, la diffusione della notifica può essere ritardata per motivi connessi alla cibersicurezza per un periodo di tempo strettamente necessario, anche nel caso in cui una vulnerabilità sia oggetto di una procedura di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555. Qualora un CSIRT decida di trattenere una notifica, informa immediatamente l'ENISA della decisione e fornisce sia una giustificazione per il trattenimento della notifica sia un'indicazione di quando diffonderà la notifica secondo la procedura di diffusione di cui al presente paragrafo. L'ENISA può sostenere il CSIRT nell'applicazione dei motivi connessi alla cibersicurezza relativamente al ritardo nella diffusione della notifica.

In circostanze particolarmente eccezionali, se il fabbricante indica nella notifica di cui all'articolo 14, paragrafo 2, lettera b):

- a) che la vulnerabilità notificata è stata attivamente sfruttata da un soggetto malintenzionato e, in base alle informazioni disponibili, non è stata sfruttata in altri Stati membri oltre a quello del CSIRT designato come coordinatore al quale il fabbricante ha notificato la vulnerabilità;
- b) che un'ulteriore diffusione immediata della vulnerabilità notificata comporterebbe probabilmente la fornitura di informazioni la cui divulgazione sarebbe contraria agli interessi essenziali di tale Stato membro; o
- c) che l'ulteriore diffusione della vulnerabilità notificata si tradurrebbe in un rischio di cibersicurezza elevato e imminente;

unicamente l'informazione dell'avvenuta notifica da parte del fabbricante, le informazioni generali sul prodotto, le informazioni sulla natura generale dello sfruttamento e l'informazione che sono stati sollevati motivi di sicurezza, devono essere rese simultaneamente disponibili a l'ENISA fino a quando la notifica completa non viene diffusa ai CSIRT interessati e all'ENISA. Se l'ENISA, sulla base di tali informazioni, ritiene che vi sia un rischio sistemico capace di incidere sulla sicurezza del mercato interno, raccomanda al CSIRT ricevente di diffondere la notifica completa agli altri CSIRT designati come coordinatori e all'ENISA stessa.

3. Dopo aver ricevuto la notifica di una vulnerabilità attivamente sfruttata in un prodotto con elementi digitali o di un incidente grave che ha un impatto sulla sicurezza di un prodotto con elementi digitali, i CSIRT designati come coordinatori forniscono alle autorità di vigilanza del mercato dei rispettivi Stati membri le informazioni notificate necessarie alle autorità di vigilanza del mercato per adempiere ai loro obblighi a norma del presente regolamento.

4. L'ENISA adotta misure adeguate e proporzionate dal punto di vista tecnico, operativo e organizzativo per gestire i rischi posti alla sicurezza della piattaforma unica di segnalazione e alle informazioni trasmesse o diffuse attraverso la stessa. Essa notifica senza indebito ritardo alla rete di CSIRT e alla Commissione qualsiasi incidente di sicurezza che incida sulla piattaforma unica di segnalazione.

5. L'ENISA, in cooperazione con la rete di CSIRT, fornisce e attua specifiche sulle misure tecniche, operative e organizzative relative all'istituzione, alla manutenzione e al funzionamento sicuro della piattaforma unica di segnalazione di cui al paragrafo 1, comprese almeno le disposizioni in materia di sicurezza relative all'istituzione, al funzionamento e alla manutenzione della piattaforma unica di

segnalazione, nonché i terminali per la notifica elettronica istituiti dai CSIRT designati come coordinatori a livello nazionale e dall'ENISA a livello di Unione, compresi gli aspetti procedurali per garantire che, qualora per una vulnerabilità notificata non siano disponibili misure correttive o di attenuazione, le informazioni su tale vulnerabilità siano condivise nel rispetto di rigorosi protocolli di sicurezza e in funzione della necessità di conoscere.

6. Qualora un CSIRT designato come coordinatore sia stato informato di una vulnerabilità attivamente sfruttata nell'ambito di una procedura di divulgazione coordinata delle vulnerabilità di cui all'articolo 12, paragrafo 1, della direttiva (UE) 2022/2555, il CSIRT designato come coordinatore che ha ricevuto per primo la notifica può ritardare la diffusione della notifica in questione attraverso la piattaforma unica di segnalazione sulla base di motivi giustificati legati alla cibersicurezza per un periodo non superiore a quello strettamente necessario e fino a quando non sia stato dato il consenso alla divulgazione dalle parti coinvolte nella divulgazione coordinata delle vulnerabilità. Tale requisito non impedisce ai fabbricanti di notificare tale vulnerabilità su base volontaria secondo la procedura di cui al presente articolo.

Fonti

[Regolamento \(UE\) 2024/2847](#)
[Guida applicazione Regolamento \(UE\) 2024/2847 \(CyberResilience Act\)](#)

Collegati

[Regolamento \(UE\) 2024/2847](#)
[Guida applicazione Regolamento \(UE\) 2024/2847 \(CyberResilience Act\)](#)
[Regolamento Macchine e Cibersicurezza / Note](#)

Matrice Revisioni

Rev.	Data	Oggetto
0.0	05.10.2026	---

Note Documento e legali

[certifico.com](#)
Testata editoriale iscritta al n. 22/2024 registro periodici Tribunale di Perugia 19.11.2024

Certifico Srl - IT | Rev. 0.0 2026
©Copia autorizzata Abbonati
ID 27230 | 05.10.2026
Permalink: <https://www.certifico.com/id/27230>
[Policy](#)

