

# Piattaforma unica di segnalazione del regolamento sulla ciberresilienza – Scheda informativa

Come notificare gli incidenti e le vulnerabilità attivamente sfruttate tramite la piattaforma unica di segnalazione

## ■ Che cosa?

A decorrere dall'11 settembre 2026, il regolamento sulla ciberresilienza impone ai fabbricanti di notificare le vulnerabilità attivamente sfruttate e gli incidenti gravi che hanno un impatto sulla sicurezza dei prodotti con elementi digitali venduti sul mercato dell'UE.

Il regolamento sulla ciberresilienza impone inoltre ai gestori di software open source di notificare tali eventi nella misura in cui sono coinvolti nello sviluppo di prodotti con elementi digitali.

## ■ Per chi?



Fabbricanti



Gestori di software open source

## ■ Quali sono i nuovi obblighi di segnalazione?

La piattaforma unica di segnalazione del regolamento sulla ciberresilienza è uno strumento online che consente ai fabbricanti e ai gestori di software open source di adempiere all'obbligo di notificare le vulnerabilità attivamente sfruttate e gli incidenti gravi. Concepita per semplificare gli obblighi di segnalazione dell'UE, la piattaforma unica di segnalazione del regolamento sulla ciberresilienza è un sistema elettronico che permette di effettuare un'unica notifica per trasmettere le

informazioni a tutte le autorità pertinenti. La piattaforma integra misure di sicurezza a tutela della riservatezza.

Ogni notifica consente di trasmettere automaticamente le informazioni al proprio gruppo di intervento per la sicurezza informatica in caso di incidente (CSIRT) nazionale che riceve per primo la notifica, agli altri CSIRT nazionali degli Stati membri in cui il prodotto con elementi digitali è disponibile e all'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

## ■ Come si individua il CSIRT nazionale al quale effettuare la notifica?

In generale, il CSIRT nazionale al quale effettuare la notifica tramite la piattaforma unica di segnalazione dipende innanzitutto dal luogo in cui si trova lo stabilimento principale. L'articolo 14, paragrafo 7, del regolamento sulla ciberresilienza fornisce informazioni dettagliate che permettono di individuare il CSIRT nazionale destinatario della notifica.

## ■ Quali eventi devono essere obbligatoriamente notificati?

- **Vulnerabilità attivamente sfruttate:** vulnerabilità presenti in prodotti con elementi digitali per le quali è noto uno sfruttamento in atto da parte di un soggetto malintenzionato, conformemente all'articolo 3, punto 42), del regolamento sulla ciberresilienza.
- **Incidenti gravi:** incidenti che hanno un impatto grave sulla sicurezza del prodotto con elementi digitali (ad esempio compromettendo la disponibilità, l'autenticità, l'integrità o la riservatezza), conformemente all'articolo 3, punto 44); i criteri di gravità sono definiti all'articolo 14, paragrafo 5.

## ■ Entro quando devono essere notificati tali eventi?

Il processo di segnalazione inizia nel momento in cui il fabbricante o il gestore di software open source viene a conoscenza dello sfruttamento attivo di una vulnerabilità o di un incidente grave. I termini da rispettare sono i seguenti:

### Preallarme



- entro **24 ore** dal momento in cui viene a conoscenza della vulnerabilità o dell'incidente.

### Notifica di vulnerabilità attivamente sfruttata/dell'incidente grave



- entro **72 ore** dal momento in cui ne viene a conoscenza, fornendo informazioni generali e una valutazione iniziale.

### Relazione finale



- Per le **vulnerabilità**: entro e non oltre **14 giorni** dalla messa a disposizione di una misura correttiva (ad esempio una patch).
- Per gli **incidenti gravi**: entro **un mese** dalla trasmissione della notifica a 72 ore della vulnerabilità attivamente sfruttata/dell'incidente grave.

## ■ Che cosa accade una volta trasmesse le notifiche?

Una volta trasmesse le notifiche, il CSIRT che riceve per primo la notifica diffonde senza indugio le informazioni agli altri CSIRT pertinenti degli Stati membri dell'UE in cui il prodotto è parimenti disponibile. La notifica è contemporaneamente resa accessibile all'ENISA.

I CSIRT nazionali condividono inoltre alcune informazioni con le rispettive autorità di vigilanza del mercato, per consentire loro di adempiere ai propri obblighi in materia di applicazione delle norme.

## ■ La diffusione delle informazioni può essere ritardata?

**Sì**, in circostanze eccezionali la diffusione delle informazioni può essere ritardata, a norma dell'articolo 16, paragrafo 2, del regolamento sulla ciberresilienza. Il regolamento delegato (UE) 2026/881 della Commissione ( ) precisa ulteriormente le condizioni alle quali la diffusione delle notifiche può essere ritardata.

## ■ Ako využiť platformu na nahlásenie?



1 Login



2 Seleziona il CSIRT nazionale



3 Completa i dati e invia

## ■ Schema del flusso di segnalazione

