PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5853 di Mercoledì 21 maggio 2025

Disponibile il database delle vulnerabilità informatiche

Il 13 marzo 2025 è stato messo in rete il data base, gestito e costantemente aggiornato dall'agenzia dell'unione europea per la cybersicurezza (ENISA), chiamato EUVD - European Union Vulnerability Database.

In attuazione di una specifica direttiva NIS2, l'agenzia dell'unione europea per la cybersicurezza-ENISA, ha finalmente attivato e messo disposizione di tutti un preziosissimo data base, che illustra le vulnerabilità presenti nei sistemi informativi, chiamato **EUVD - European Union Vulnerability Database**.

Il pregio di questo documento sta nel costante aggiornamento, in modo da mettere a disposizione degli esperti informatici un prezioso strumento di profilassi e messa sotto controllo di debolezze informatiche.

Questo data base offre delle informazioni aggregate, affidabili ed aggiornate su vulnerabilità informatiche, che possono essere presenti in prodotti e servizi ITC. Il bello di questo data base sta nel fatto che, insieme alla vulnerabilità, vengono anche illustrate le misure che possono mettere sotto controllo rapidamente la vulnerabilità stessa.

Questa attività, decisamente impegnativa è stata attivata da ENISA per attuare una prescrizione della direttiva NIS 2-Network and Information Security Directive 2.

Da oggi, gli esperti di sicurezza informatica, che operano nel contesto dell'unione europea, hanno a disposizione un documento utilissimo, che però accresce in maniera significativa la responsabilità di questi esperti, ove l'azienda, che essi assistono, rimanga vittima di una vulnerabilità, già pubblicizzata su questo data base.

Questo data base è stato messo a disposizione del pubblico, in modo che possa essere data la massima possibile diffusione a possibili debolezze informatiche, che vengono successivamente sfruttate dai criminali informatici.

Può essere oltremodo importante, per i fornitori di servizi informatici, tenersi costantemente aggiornati e, come raccomandazione supplementare, può essere opportuno che nei contratti per la fornitura di servizi informatici venga esplicitamente fatto riferimento al fatto che il fornitore di servizi informatici si impegna a consultare costantemente questo data

base, attivando le misure di contrasto e mitigazione, che nel data base sono illustrate.

Il database è articolato in tre diverse presentazioni, che fanno riferimento, rispettivamente,

- a vulnerabilità critiche,
- a vulnerabilità già note, e
- a vulnerabilità già coordinate livello europeo.

Queste ultime vulnerabilità sono state già identificate e inserite nel database dal noto organismo di sicurezza informatica europeo CSIRT-Computer Security Incident Response Team.

Un tipico campo che illustra una possibile debolezza, è articolato in tre fasi:

- una descrizione della vulnerabilità,
- una illustrazione dei servizi o prodotti ITC che possono essere coinvolti nella vulnerabilità, insieme ad informazioni afferenti alla gravità della vulnerabilità e al modo con cui essa può essere utilizzata dai criminali informatici,
- informazioni su possibili esistenti sistemi di messa contro controllo od indicazione aggiuntive, tese allo stesso obiettivo.

Al proposito, può essere utile far presente ai lettori che dal settembre 2026 diventerà obbligatorio per tutti i fabbricanti, che hanno conoscenza di una vulnerabilità informatica, di comunicare tale situazione a tutti i loro clienti e, meglio ancora, al grande pubblico. Queste vulnerabilità fanno evidentemente riferimento sia vulnerabilità hardware, sia software.

I lettori possono cliccare sul link apposito, in modo da accedere direttamente al database, e verificare non solo l'elenco delle vulnerabilità, ma anche il livello di aggiornamento del database stesso.

In fase di scrittura di questo articolo, ci siamo collegati a questo sito alle 11:01 del 15 maggio 2025 ed abbiamo rilevato che l'ultima vulnerabilità ivi illustrata risaliva a quattro ore prima!

Adalberto Biasiotti