681 vulnerabilità nei sistemi di controllo industriale nel 2022

Lug 21, 2022 Redazione news News, RSS, Vulnerabilità 0

Il 53% delle vulnerabilità esaminate richiede una patch software, il 34% un aggiornamento del firmware e il 12% un aggiornamento dei protocolli. Il 13% potrebbe non essere mai risolto

Secondo un'analisi condotta da SynSaber, società di monitoraggio delle reti e degli asset industriali, nella prima metà del 2022 sono state **rese note 681 vulnerabilità di sistemi di controllo industriale (ICS) da parte della Cybersecurity and Infrastructure Security Agency (CISA) statunitense**.

Il numero è leggermente più alto rispetto a quello della prima metà del 2021 (637) e le effettive vulnerabilità divulgate nel periodo potrebbero essere di più, dato che la CISA non pubblica avvisi per tutte le falle.

Per il 13% delle vulnerabilità del 2022 non sono attualmente disponibili patch o rimedi da parte del fornitore e potrebbero non essere mai risolte. **Quando non esiste una soluzione e il fornitore dichiara che il bug non verrà mai risolto, si parla di "Forever-day Vulnerability".**

In generale, **anche se è disponibile una patch del software o del firmware, le aziende devono collaborare con il fornitore dell'OEM** (original equipment manufacturer o produttore di apparecchiature originali) interessato e attendere l'approvazione ufficiale per eseguire la patch.

Ai sistemi di controllo industriale si applicano infatti complicati vincoli di interoperabilità e garanzia. Il fatto che esista una patch non significa inoltre che un'organizzazione possa applicarla immediatamente. **Oltre a gestire le restrizioni degli OEM, le aziende devono determinare il rischio operativo** e seguire le politiche e le procedure interne di gestione della configurazione.

Il **53%** delle vulnerabilità esaminate richiede una **patch**

software, il **34%** un **aggiornamento del firmware** e il **12%** un **aggiornamento dei protocolli**.

Al **22,32% delle vulnerabilità** rese pubbliche dalla CISA nel primo semestre del 2022 è stata assegnata una **valutazione di gravità "critica"** e al **42,44%** una **valutazione di "gravità elevata"** in base al punteggio CVSS.

SynSaber sottolinea però l'importanza anche di altri parametri che rendono le vulnerabilità più o meno pericolose per le aziende. **Il 29% delle falle segnalate richiede che l'utente (operatore) compia un'azione per essere sfruttato.**

Il report sottolinea inoltre che, nelle reti industriali, accesso significa controllo. **154 (22,61%) delle vulnerabilità segnalate richiedono l'accesso locale o fisico al sistema per essere sfruttate**, il che le rende a rischio inferiore. Se si dispone di un accesso locale/fisico, inoltre, spesso non è necessario alcun exploit per azioni malevole.

Lo studio indica anche che **il volume delle vulnerabilità non è destinato a diminuire** e conclude: "È importante che i proprietari degli asset e coloro che difendono le infrastrutture critiche capiscano quando sono disponibili soluzioni e come queste debbano essere implementate e classificate in base alle priorità.

Limitarsi a guardare il volume dei CVE segnalati può far sentire i proprietari delle risorse sopraffatti, ma **le cifre sembrano meno scoraggianti quando si capisce quale percentuale di CVE è pertinente e perseguibile** e quali invece rimarranno "forever-day vulnerability", almeno per il momento".

Autenticazione debole alla base dell'80% delle violazioni finanziarie Nasce la startup per la sicurezza dell'intelligenza artificiale

Articoli correlati

Altro in questa categoria