AGENZIA STAMPA QUOTIDIANA NAZIONALE
Prima Pagina News

Tecnologia - *Claroty, Team82: il 38% dei sistemi cyber-fisici più a rischio trascurato da tradizionali metodi di gestione vulnerabilità*

Roma - 07 mag 2024 (Prima Pagina News) **Claroty lancia Cps-native Exposure Management, una soluzione progettata appositamente per rivelare e dare priorità ai rischi che incombono sui sistemi critici.**

Claroty ha presentato oggi dati allarmanti che rivelano che il 38% delle risorse CPS più a rischio viene trascurato dai tradizionali metodi di gestione delle vulnerabilità, creando così un preoccupante punto cieco all'interno della sicurezza pronto per essere sfruttato dai cyber criminali. Per risolvere questo problema, Claroty ha progettato una soluzione completa per gestire l'esposizione dei CPS a tali minacce e che consente alle aziende di ridurre al minimo la superficie di attacco, dando priorità ai rischi immediati. Le aziende non hanno la piena consapevolezza di quali sono le esposizioni più rischiose Per comprendere la portata dell'esposizione e i rischi associati agli ambienti CPS, Team82, il pluripremiato gruppo di ricercatori Claroty, ha analizzato i dati relativi a oltre 20 milioni di tecnologie operative (OT), dispositivi medici connessi (IoMT), IoT e IT in ambienti CPS. La ricerca si è concentrata sulle risorse "ad alto rischio", dotate di una connessione internet poco sicura e che presentavano almeno una vulnerabilità sfruttata nota (KEV). I ricercatori hanno definito "ad alto rischio" tutti gli asset che presentavano un'elevata probabilità di essere sfruttati e il cui attacco sarebbe stato di particolare impatto, sulla base di una combinazione di fattori di rischio, come lo stato di fine vita, la comunicazione con protocolli non sicuri, le vulnerabilità note, l'utilizzo di password deboli o predefinite, i dati PII o PHI, le conseguenze in caso di guasto e molti altri ancora. I principali risultati hanno evidenziato che: · Il 20% dei sistemi OT e IoMT ha un punteggio CVSSv3.1 pari o superiore a 9.0, una valutazione che rispecchia il tradizionale approccio di gestione delle vulnerabilità basato esclusivamente sul Common Vulnerability Scoring System version 3.1. Per la maggior parte delle aziende, però, il numero di vulnerabilità indicato dal CVSSv3.1 è troppo elevato e richiede molte risorse per essere affrontato in modo realistico, soprattutto per i CPS con finestre limitate di patching. Inoltre, non fornisce alcuna indicazione sulla priorità da dare a tali vulnerabilità. · L'1,6% degli OT e IoMT è definito "ad alto rischio", ha una connessione Internet poco sicura e contiene almeno una KEV, che insieme rappresentano i principali fattori di esposizione e un pericolo reale e imminente per le aziende. Il che si traduce in decine di migliaia di asset CPS "ad alto rischio" che possono essere accessibili da remoto ai malintenzionati e che contengono vulnerabilità attivamente sfruttati. · Di questi dispositivi OT e IoMT ad altissimo rischio, il 38% non ha un punteggio CVSS pari o superiore a 9.0. Per questo motivo vengono spesso trascurati dai tradizionali metodi di gestione delle vulnerabilità, ma possono essere ampiamente sfruttati e presi di mira dai cyber criminali, rappresentando così

un “punto cieco” molto rischioso per le organizzazioni. "Quando si misura il rischio associato a risorse iper-esposte, utilizzate per controllare sistemi come la rete elettrica o per fornire cure salvavita ai pazienti, è importante comprendere tutte le implicazioni di un punteggio superiore allo zero”, ha dichiarato Amir Preminger, Vice President of Research del Team82 di Claroty. "Le aziende devono adottare un approccio olistico nella gestione dell'esposizione, che gli permetta di concentrarsi sugli asset “ad alto rischio” all’interno dei propri ambienti. Questo perché anche se riuscissero in qualche modo a padroneggiare il compito impossibile di affrontare ogni singola vulnerabilità CVSS 9.0+, non riuscirebbero comunque ad individuarci circa il 40% delle minacce più pericolose". Colmare questo divario con CPS-native Exposure Management di Claroty Secondo Gartner®, "i leader della sicurezza sono sempre alla ricerca dei framework e degli strumenti più adatti a ridurre i rischi legati alla cybersecurity. Ciò include il passaggio da un approccio esclusivamente preventivo a controlli preventivi più maturi, in grado di ottimizzare la strategia e dotati di capacità di rilevamento e risposta. Gli approcci utilizzati fino a poco tempo fa relativi alla gestione della superficie di attacco, infatti, non sono più in grado di tenere il passo con la diffusione del digitale, soprattutto in un’epoca in cui le aziende non possono contrastare ogni singola vulnerabilità e devono definire quelle a cui dare maggiore priorità. La gestione continua dell'esposizione alle minacce (CTEM) è un approccio sistemico pragmatico ed efficace per affinare continuamente tali priorità, trovando il giusto compromesso per una strategia di sicurezza il più efficace possibile". Per soddisfare le esigenze in continua evoluzione delle aziende manifatturiere, sanitarie e di altre infrastrutture critiche, Claroty ha introdotto una soluzione completa per la gestione dell'esposizione dei CPS, che si allinea al framework CTEM di Gartner. La soluzione consente ai clienti di comprendere la loro attuale posizione di rischio CPS, di organizzare le proprie risorse per migliorarla in modo più efficiente ed efficace e, infine, di accelerare il percorso verso la maturità della sicurezza CPS, indipendentemente dal punto di partenza. Le principali funzionalità includono: · Inclusione dei dispositivi CPS nei programmi di gestione dell'esposizione: sfruttare metodi multipli per la raccolta dei dati e calcoli del rischio personalizzati, che tengano conto del valore aziendale relativo ai diversi aspetti del processo produttivo. Questo approccio pone le basi per lo scoping della rete, sia per proteggere aree che potrebbero rappresentare dei punti ciechi per le soluzioni tradizionali, sia per analizzare i risultati operativi quando si stabilisce la priorità dei controlli di sicurezza. · Individuazione e valutazione delle vulnerabilità dei CPS: identificazione e profilazione di tutte le risorse CPS, utilizzando metodi di individuazione altamente flessibili, tra cui Claroty Edge e gli SBOM associati, mappando i percorsi di comunicazione e l'utilizzo del protocollo, attribuendo vulnerabilità e monitorando le minacce, ottenendo punteggi di rischio basati su un metodo trasparente e un quadro di rischio personalizzato in modo univoco. · Supporto alla definizione delle priorità per i processi CPS critici: ricevere raccomandazioni attuabili che diano priorità agli sforzi da realizzare in base a risultati quantificati, definiti da specifici vettori di attacco e dalla loro probabilità di essere sfruttati, dall'impatto in caso di sfruttamento e dai controlli compensativi applicati. · Convalida sicura degli scenari di esposizione: spingersi oltre alla semplice gestione delle vulnerabilità, indagando sull'exploitability grazie all’utilizzo di file VEX e ulteriori tattiche di scoperta, come la scansione attiva o la consulenza degli OEM per convalidare le valutazioni del rischio e

abilitare le corrette tecniche di remediation. · Semplificare la remediation e la mobilitazione del programma: integrazione con le soluzioni di cybersecurity e gestione degli asset IT/OT leader del settore per semplificare i processi di gestione del rischio esistenti e mobilitare la gestione dell'esposizione CPS. "Adottare un approccio concentrato sulle sole vulnerabilità non aiuta le aziende a focalizzarsi su ciò che conta di più, ma fa sì che le reali esposizioni, in grado di mettere a rischio sicurezza e disponibilità, vengano trascurate", ha dichiarato Grant Geyer, Chief Product Officer di Claroty. "La riduzione del rischio richiede l'evoluzione da un programma tradizionale di gestione delle vulnerabilità a un programma di gestione delle esposizioni più mirato e dinamico, che tenga conto delle caratteristiche e delle complessità uniche degli asset CPS, dei vincoli operativi e ambientali, della tolleranza al rischio dell'azienda e dei risultati che si desiderano raggiungere con il programma di rischio informatico CPS".

(Prima Pagina News) Martedì 07 Maggio 2024

Verbalia Comunicazione S.r.l. Società Editrice di PRIMA PAGINA NEWS
Registrazione Tribunale di Roma 06/2006 - P.I. 09476541009
Iscrizione Registro degli Operatori di Comunicazione n. 21446

Sede legale : Via Costantino Morin, 45 00195 Roma
Redazione Tel. 06-45200399 r.a. - Fax 06-23310577
E-mail: redazione@primapaginanews.it