TEAM82 DI CLAROTY:
IL PROBLEMA DELLA CONNETTIVITÀ DELL'IoT AL CLOUD E L'ESPOSIZIONE DEI DISPOSITIVI OvrC ALL'HIJACKING

Milano, 20 novembre 2024. Il Team82 di Claroty ha condotto un'analisi approfondita sulla sicurezza della piattaforma cloud OvrC, utilizzata da aziende e privati per la gestione remota dei dispositivi IoT. Lo studio ha individuando dieci vulnerabilità che, se combinate, consentono agli aggressori di eseguire un codice da remoto sui dispositivi connessi al cloud OvrC. Queste falle interessano sia OvrC Pro che OvrC Connect. Otto delle dieci vulnerabilità sono state risolte con aggiornamenti rilasciati a maggio 2023 tramite l'avviso ICSA-23-136-01, mentre le due restanti sono state corrette recentemente con un ulteriore aggiornamento. L'avviso completo pubblicato da CISA è disponibile al seguente link.

È bene ricordare che quando si parla di sicurezza informatica dei dispositivi IoT esistono alcune problematiche ricorrenti: i produttori di questi device connessi, infatti, tendono a trascurarne la sicurezza in favore dello sviluppo di nuove funzionalità, ponendo in secondo piano solidi metodi di autenticazione o controlli di accesso efficaci. I dispositivi IoT utilizzano spesso protocolli deboli o obsoleti per la comunicazione con il cloud, senza adottare soluzioni di crittografia a protezione dei dati.

Questo approccio è alimentato dalla breve durata del ciclo di vita dei dispositivi IoT rispetto a quelli IT o OT, nonché da fattori come costi, complessità e carenza di competenze specifiche. Tuttavia, l'incremento di dispositivi connessi e gestiti tramite piattaforme cloud crea un ambiente fertile per gli attacchi informatici, mettendo a rischio servizi essenziali, dati sensibili e attività aziendali.

In questo contesto si inserisce la ricerca del Team82, che ha esaminato la piattaforma OvrC cloud , una soluzione per la gestione e il monitoraggio remoto basata su cloud. Acquisita nel 2014 da SnapOne, azienda statutitense specializzata in automazione, in particolare per dispositivi IoT smart, OvrC consente la configurazione, il monitoraggio e la risoluzione dei problemi dei dispositivi tramite un'app mobile o un'interfaccia utente basata su websocket. La piattaforma supporta dispositivi come endpoint di automazione domestica, interruttori smart, videocamere, router e molto altro. Secondo un webinar del 2020 di OvrC, circa 9,2 milioni di dispositivi erano monitorati dalla piattaforma. È quindi plausibile che le vulnerabilità segnalate abbiano interessato circa 10 milioni di dispositivi a livello globale.

La ricerca ha identificato dieci vulnerabilità sia in OvrC Pro, che offre visibilità, diagnosi e dati per la gestione remota dei dispositivi, sia in OvrC Connect, l'app mobile per la configurazione e il troubleshooting. Attraverso queste falle gli aggressori potrebbero accedere ai dispositivi, controllarli e comprometterne il funzionamento. L'elenco di tali dispositivi comprende alimentatori smart, videocamere, router, sistemi di automazione domestica e molto altro.

Gli attacchi sfruttano la possibilità di aggirare misure di sicurezza come firewall e NAT, consentendo di profilare i dispositivi, rivendicarne il controllo, elevare i privilegi ed eseguire un codice arbitrario. Tali problematiche derivano da un'attenzione insufficiente all'interfaccia dispositivo-cloud, un fenomeno comune anche a molte altre piattaforme IoT. Questi problemi spaziano da controlli di accesso carenti, elusione dell'autenticazione, errori nella validazione degli input, credenziali hardcoded e vulnerabilità di esecuzione remota del codice.

Con il crescente aumento di dispositivi connessi ogni giorno e la gestione cloud ormai predominante per configurare e accedere ai servizi, è più che mai fondamentale che i produttori e i fornitori di servizi cloud investano nella sicurezza per proteggere connessioni e dispositivi. È, inoltre, importante sottolineare come le vulnerabilità e le debolezze identificate dal Team82 non siano un'eccezione, ma sintomatiche di un settore che ancora fatica a bilanciare innovazione e cybersecurity, lasciando campo aperto ai malintenzionati per sfruttarne le debolezze.

Per maggiori informazioni e approfondimenti, l'intera ricerca condotta dal Team82 di Claroty è disponibile al seguente link.

Claroty

Claroty ha ridefinito la protezione dei sistemi cyber-fisici con una piattaforma unica, con un forte focus sul settore, creata per proteggere le infrastrutture mission-critical. La piattaforma Claroty offre una visibilità più approfondita delle risorse e la più ampia gamma di soluzioni progettate per CPS sul mercato, che comprende gestione dell'esposizione, protezione della rete, accesso sicuro e rilevamento delle minacce, sia nel cloud con Claroty xDome che on-premise con Claroty CTD. Supportata da molteplici alleanze tecnologiche, la piattaforma Claroty consente alle aziende di ridurre efficacemente il rischio CPS, con un time-to-value più rapido e un costo totale di proprietà contenuto. Le soluzioni Claroty vengono distribuite da centinaia di organizzazioni in migliaia di siti in tutto il mondo. La società ha sede a New York e filiali in Europa, Asia-Pacifico e America Latina. Per maggiori informazioni: www.claroty.com.

Ufficio Stampa
Meridian Communications Srl
Via Cuneo, 3 – 20149 Milano Tel. +39 02 48519553

Silvia Ceriotti	335 7799816	silvia.ceriotti@meridiancommunications.it
Viviana Bandieramonte	329 4776937	viviana.bandieramonte@meridiancommunications.it
Ilaria Malgrati	339 2143042	ilaria.malgrati@meridiancommunications.it