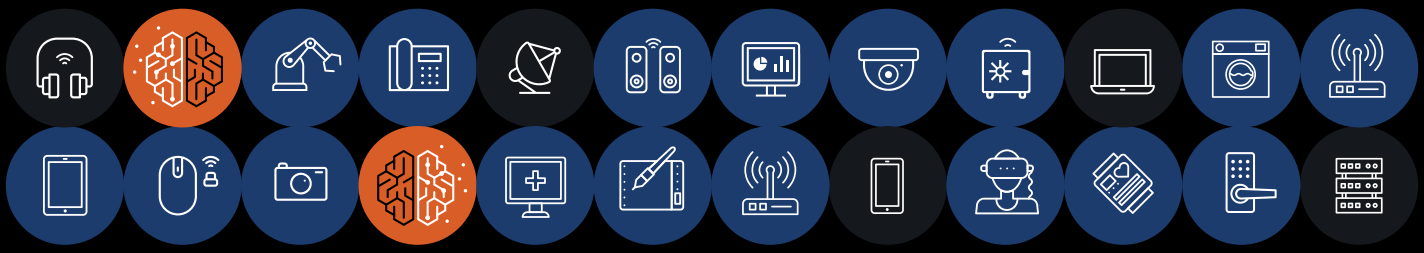
FORESCOUT
Active Defense for the Enterprise of Things™

AMNESIA:33

Sintesi della ricerca



- Forescout Research Labs ha dato vita a Project Memoria, **un'iniziativa** che ha lo scopo di condurre lo **studio più approfondito mai realizzato sulla sicurezza degli stack TCP/IP**. L'obiettivo di Project Memoria è analizzare in profondità i bug più comuni alla base delle vulnerabilità degli stack TCP/IP, individuare le minacce che rappresentano per l'azienda estesa e scoprire come mitigare i rischi.
- **AMNESIA:33** è il primo studio pubblicato nell'ambito di Project Memoria. Contiene i risultati di un'analisi sulla sicurezza condotta su sette **stack TCP/IP open source** e riporta le **33 nuove vulnerabilità** rilevate in quattro dei sette stack analizzati nonché utilizzati dai principali fornitori di dispositivi IoT, OT e IT del mercato.
- **Quattro delle vulnerabilità indicate nello studio AMNESIA:33 hanno una gravità critica** e sono potenzialmente sfruttabili per l'esecuzione di codice da remoto su determinati dispositivi. Sfruttando queste vulnerabilità un criminale informatico può assumere il controllo di un dispositivo trasformandolo in punto di accesso a una rete in cui sono presenti dispositivi connessi a Internet, impiegandolo come punto di partenza per una serie di movimenti laterali o come strumento di persistenza nella rete attaccata o ancora utilizzandolo come obiettivo finale di un attacco. Per le imprese il rischio è che gli attacchi criminali violino l'intera rete aziendale o pregiudichino la continuità operativa. Per i consumatori il rischio è che i loro dispositivi IoT siano dirottati e coinvolti in campagne di attacco di grande portata, come le botnet, a loro insaputa.

Oltre 150

FORNITORI INTERESSATI

forescout.com/amnesia33/ info-italia@forescout.com Tel. (internazionale) +1-408-213-3191

- Le vulnerabilità esaminate in AMNESIA:33 riguardano **vari stack TCP/IP open source non riconducibili a un'unica azienda**. Ciò significa che una vulnerabilità ha la tendenza a **diffondersi in modo rapido e silenzioso** interessando diversi codebase, team di sviluppo, aziende e prodotti, il che rappresenta una difficoltà non indifferente per le attività di riparazione.
- Si stima che oltre 150 fornitori e milioni di dispositivi siano soggetti alle vulnerabilità di AMNESIA:33. **Rimane tuttavia difficile valutare il pieno impatto** delle vulnerabilità di AMNESIA:33 perché gli stack vulnerabili individuati sono largamente diffusi (diversi dispositivi IoT, OT e IT in vari mercati verticali), sono caratterizzati da un'elevata modularità (i componenti, le funzionalità e le impostazioni sono presenti in diverse combinazioni e codici sorgente utilizzati per sviluppare progetti diversi) e sono incorporati in profondità all'interno di sottosistemi senza essere documentati. Queste stesse caratteristiche rendono l'eliminazione delle vulnerabilità estremamente difficile.
- Gli stack TCP/IP soggetti alle vulnerabilità di AMNESIA:33 sono presenti in sistemi operativi di dispositivi integrati, SoC o circuiti integrati, apparecchiature di rete, dispositivi OT e una miriade di dispositivi IoT aziendali e consumer.
- Dal momento che supportano le funzionalità di comunicazione di base, gli stack TCP/IP sono un componente basilare di qualsiasi dispositivo con connessione IP - IoT e OT compresi. Una falla nella sicurezza di uno stack TCP/IP può rivelarsi estremamente pericolosa perché il codice di questi componenti può essere utilizzato per **elaborare *ogni singolo* pacchetto di rete in entrata che arriva al dispositivo**. In pratica, alcune di queste vulnerabilità dello stack TCP/IP consentono di sfruttare persino i dispositivi che sono semplicemente collegati alla rete e che non sono preposti all'esecuzione di alcuna applicazione specifica.
- Molte delle vulnerabilità evidenziate in **AMNESIA:33** sono il risultato di pratiche di sviluppo software scorrette, come l'assenza di una basilare convalida degli input. Sono legate prevalentemente alla **corruzione della memoria** e possono provocare problemi di tipo **denial of service, divulgazione di informazioni** o **esecuzione di codice da remoto**.
- In ragione delle difficoltà che l'identificazione e la riparazione dei dispositivi vulnerabili comportano, la gestione delle vulnerabilità degli stack TCP/IP sta diventando un problema per chi si occupa di sicurezza. Per contenere i rischi causati da queste vulnerabilità, consigliamo di **adottare una soluzione in grado di assicurare una visibilità completa e granulare nei dispositivi**, di attivare il monitoraggio delle comunicazioni di rete e di isolare i dispositivi o i segmenti di rete vulnerabili.

Vedere non basta. Bisogna proteggere.

Contattaci oggi stesso per difendere subito il tuo ambiente EoT.

Scarica il report completo (in inglese): Leggi la nostra ricerca e scopri le tecniche di mitigazione che puoi mettere in atto.

Scarica il white paper (in inglese): Scopri come Forescout può aiutarti a difenderti attivamente dalle vulnerabilità di AMNESIA:33 e quali sono le sei best practice che mettono al sicuro la tua attività.

Guarda il webinar (in inglese): I nostri esperti descrivono i punti salienti della ricerca.

forescout.com/amnesia33/ info-italia@forescout.com Tel. (internazionale) +1-408-213-3191

FORESCOUT
Active Defense for the Enterprise of Things™

Forescout Technologies, Inc.
190 W Tasman Dr.
San José, CA 95134 Stati Uniti

E-mail info-italia@forescout.com
Tel. (internazionale) +1-408-213-3191
Assistenza +1-708-237-6591

Maggiori informazioni su Forescout.it