Vulnerabilità scoperta nel sistema di presentazione wireless ClickShare di Barco

Author : Redazione

Date : 14 Gennaio 2020

Gli esperti di sicurezza della divisione F-Secure Consulting di F-Secure hanno scoperto diverse vulnerabilità che possono essere sfruttate in un noto sistema di presentazione wireless. Gli attaccanti potrebbero utilizzare queste falle per intercettare e manipolare le informazioni durante le presentazioni, rubare password e altre informazioni riservate, installare backdoor e altri malware.

Il sistema di presentazione wireless ClickShare di Barco è uno strumento di collaborazione che aiuta gruppi di utenti a presentare contenuti da diversi dispositivi. ClickShare è un sistema di presentazione wireless con una quota di mercato del 29% secondo il rapporto "Global Wireless Presentation Solutions 2019" di FutureSource Consulting.

Dmitry Janushkevich di F-Secure Consulting, un consulente senior specializzato in sicurezza hardware, afferma che la popolarità di questi strumenti user-friendly li rende obiettivi logici per un attacco, e questo ha spinto il suo team a indagare più a fondo.

"*Il sistema è così pratico e facile da usare che le persone non riescono a trovare alcun motivo per diffidare. Ma la sua ingannevole semplicità nasconde meccanismi interni estremamente complessi e questa complessità rende difficile la sicurezza*", spiega Janushkevich. "*Gli oggetti di uso quotidiano di cui le persone si fidano senza pensarci due volte sono i migliori obiettivi per gli attaccanti e, dato che questi sistemi sono così popolari tra le aziende, abbiamo deciso di provare ad attaccarli per vedere cosa potevamo imparare*."

Janushkevich e i suoi colleghi di F-Secure Consulting hanno studiato il sistema Clickshare su base on-and-off per diversi mesi dopo aver notato la sua popolarità durante gli assessment del Red Team. Hanno scoperto molteplici falle sfruttabili, 10 delle quali hanno identificatori CVE (Common Vulnerabilities and Exposures). Queste falle facilitano una varietà di attacchi, tra cui l'intercettazione di informazioni condivise attraverso il sistema, l'utilizzo del sistema per installare backdoor o altro malware sui computer degli utenti e il furto di informazioni e password.

Sebbene lo sfruttamento di alcune vulnerabilità richieda l'accesso fisico, altre possono essere eseguite in remoto se il sistema utilizza le impostazioni predefinite. Inoltre, Janushkevich afferma che l'esecuzione degli exploit può essere eseguita rapidamente da un abile attaccante con accesso fisico (possibilmente mentre si finge un addetto alle pulizie o un impiegato), consentendogli di compromettere in modo evidente il dispositivo.

"*Gli obiettivi primari dei nostri test erano eseguire il backdoor del sistema in modo da poter compromettere i presentatori e rubare le informazioni così come venivano presentate. Sebbene sia stato difficile superare il perimetro, siamo riusciti a trovare più falle dopo aver ottenuto l'accesso e sfruttarle è stato facile una volta che abbiamo appreso di più sul sistema*", spiega Janushkevich. "*Per un attaccante questo è un modo rapido e pratico per compromettere un'azienda e le organizzazioni devono informarsi sui rischi associati*."

F-Secure Consulting ha condiviso le sue ricerche con Barco il 9 ottobre 2019 e le due società hanno lavorato insieme in uno sforzo di divulgazione coordinato. Barco ha pubblicato una release del firmware sul proprio sito web per mitigare le vulnerabilità più critiche. Tuttavia, molti dei problemi riguardano componenti hardware che richiedono una manutenzione fisica da affrontare e che è improbabile che vengano risolti.

"*Questo caso evidenzia quanto sia difficile proteggere i dispositivi 'smart'. I bug nel silicio, nella progettazione e nel software embedded possono avere effetti negativi di lunga durata sia sul vendor che sugli utenti, minando la fiducia che riponiamo in questi dispositivi*", afferma Janushkevich.

F-Secure Consulting opera in quattro continenti in 11 Paesi diversi. Fornisce servizi di sicurezza informatica su misura per soddisfare le esigenze di banche, servizi finanziari, aziende di aviazione, spedizione, vendita al dettaglio, assicurazioni e altre organizzazioni che lavorano in settori altamente presi di mira. I dettagli sulla ricerca sono disponibili in un post sul blog di F-Secure Labs. Ulteriori informazioni su F-Secure Consulting sono disponibili qui.