USBAnywhere: raffica di bug nei server Supermicro

Set 03, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le falle di sicurezza permettono di violare i sistemi di autenticazione e montare un'unità USB virtuale in remoto sui sistemi.

La virtualizzazione è un'arma a doppio taglio. Soprattutto quando si parla della possibilità di virtualizzare un'unità o un dispositivo USB attraverso un servizio remoto. A scoprirlo, in queste ore è **Supermicro**, i cui server basati su piattaforma **X9**, **X10** e **X11** risultano essere vulnerabili a un attacco remoto che sfrutta una serie di falle di sicurezza nei **Baseboard Management Controller (BMC)** utilizzati per la loro gestione in remoto.

Come si legge nel report pubblicato da **Eclypsium**, il fulcro del problema risiede proprio nei BMC utilizzati sui server Supermicro, che mettono a disposizione un sistema per utilizzare dispositivi USB virtuali attraverso un protocollo accessibile attraverso la porta TCP 623.



Secondo i ricercatori, infatti, il sistema che gestisce l'accesso in remoto ha almeno quattro problemi. Il primo riguarda **la possibilità di accedere attraverso username e password in chiaro**, il secondo ha invece a che fare con la gestione del traffico, che in buona parte non è protetto da crittografia.

Come se non bastasse, c'è il fatto che il sistema crittografico utilizza **un algoritmo debole (RC4)** e una chiave predefinita integrata nel firmware del BMC. Il quarto e ultimo punto (ma questo riguarda solo i server su piattaforma X10 e X11) riguarda un bug che consente, in pratica, di aggirare il sistema di autenticazione.

Insomma: secondo i ricercatori di Eclypsium, un pirata informatico avrebbe gioco facile a individuare un server i cui servizi BMC sono accessibili in remoto (**nel report si spiega che su Internet ce ne sarebbero più di 47.000**) e "montare" un qualsiasi dispositivo USB virtuale per poi utilizzarlo per installare malware o assumere il controllo della macchina.

[embedded content]

Gli aggiornamenti del firmware per le piattaforme Supermicro interessate sono già disponibili sul sito del produttore, ma i ricercatori indicano nel documento anche alcune tecniche di mitigazione che permettono di ridurre il rischio di un attacco.

Prima tra tutte quella di evitare di esporre direttamente su Internet l’accesso ai BMC, che rappresenta in ogni caso un potenziale fattore di rischio.

Condividi l’articolo

Gli exploit per Android valgono più di quelli per iOS Ecco i siti che hanno fatto strage di dispositivi iOS

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/09/03/usbanywhere-raffica-di-bug-nei-server-supermicro/