Thunderclap: il pericolo arriva dalle periferiche

Feb 28, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Un nuovo bug consente di sfruttare il collegamento Thenderbolt per avviare l'esecuzione di codice con i massimi livelli di privilegi.

È vero che richiede un accesso "fisico" al computer, ma la nuova vulnerabilità scoperta dai ricercatori della **University of Cambridge, Rice University e SRI International** è abbastanza grave da far suonare più di un campanello di allarme nel settore della sicurezza.

Battezzata con il nome di **Thunderclap**, la falla di sicurezza fa leva su un bug nell'interfaccia **Thunderbolt**, sviluppata da Intel e Apple e introdotta nel 2011 in numerosi modelli di computer.

L'interfaccia Thunderbolt è pensata per garantire connessioni con una larghezza di banda superiore e per un certo periodo ha sfruttato **Mini DisplayPort**. Recentemente, però, Thunderbolt ha trovato cittadinanza anche con l'introduzione delle porte **USB Type-C**.

Foto di brettferdosi CC 4.0

La vulnerabilità, nel dettaglio, sfrutta l'accesso alla funzionalità **Direct Memory Access (DMA)** delle periferiche. Semplificando: una modalità di accesso alla memoria che non è supervisionata dal sistema operativo.

Sfruttando questa tecnica, un pirata informatico può iniettare qualsiasi tipo di codice aggirando i sistemi di sicurezza. L'unico argine a questa possibilità è l'intervento dei sistemi **IOMMU (Input-Output Memory Management Unit)** che possono impedire l'accesso ai dati sensibili in memoria alle periferiche non riconosciute.

Il problema è che IOMMU ha un impatto non indifferente sulle prestazioni e, di conseguenza, è spesso disattivato come impostazione predefinita.

Ma qual è il rischio nella pratica? Lo scenario è quello di un attacco portato inducendo la vittima a collegare al suo computer una periferica infetta. Un quadro, quindi, che fa pensare immediatamente ad azioni "mirate" nell'ambito dello

spionaggio di stato, come si vede spesso nei film di spionaggio.

Come fanno notare molti esperti di sicurezza, però, non è da escludere il rischio che si verifichi un’infezione a livello **supply chain**, cioè che prende di mira i sistemi di uno dei produttori di periferiche. La casistica, in questo senso, è già abbastanza ricca e giustifica i timori dei ricercatori per un’ipotesi del genere.

In alternativa, un eventuale malware che sfrutta ThunderClap potrebbe essere diffuso attraverso la compromissione dei sistemi di aggiornamento del firmware, che in molti casi è possibile anche a causa dell’assenza di controlli adeguati nell’autenticazione delle connessioni in remoto per gli aggiornamenti.

Quale che sia lo scenario di riferimento, la nuova vulnerabilità arricchisce l’arsenale dei pirati informatici e pone nuovi problemi a livello delle policy (per esempio a livello aziendale) nella gestione dell’hardware.

Please follow and like us:

ExSpectre: l’esecuzione speculativa nasconde i malware agli antivirus

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/02/28/thunderclap-il-pericolo-arriva-dalle-periferiche/