Microsoft al lavoro per risolvere 25 bug di Windows

Apr 03, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Le falle di sicurezza sono collegate al famigerato WIN32K. Gli sviluppatori avrebbero già approntato le patch per le prime 11 falle di sicurezza.

Tempo di straordinari per gli sviluppatori **Microsoft**, che si trovano a fronteggiare una raffica di vulnerabilità di **Windows** (sono la bellezza di 25) scoperte dal ricercatore di sicurezza israeliano **Gil Dabah**.

Il perno di tutta la vicenda è rappresentato da **WIN32K**, un componente di Windows dedicato alla gestione dell'interfaccia utente per le architetture a 32 bit di Windows.

Il componente, in circolazione da molto (troppo) tempo, è stato mantenuto nelle varie versioni di Windows (anche a 64 bit) per garantire la compatibilità con le vecchie applicazioni e interagisce tra interfaccia, driver e il Kernel.

Il problema, spiega Dabah nel suo report, è che l'uso di WIN32K richiede un ampio utilizzo di richiami (callback) dal livello Kernel a quello in modalità utente. Una procedura che, a partire dal 2010, ha evidenziato una serie di problemi e, in particolare, la possibilità di portare un attacco battezzato con il nome di **use-after-free o UAF**.

La tecnica fa leva su un errore nella gestione degli oggetti in memoria e consente, in pratica di eseguire comandi da parte di un utente non autenticato. **In altre parole: apre la strada alla compromissione della macchina**.

Negli ultimi 12 mesi, il ricercatore si è dedicato a questo problema e ha individuato le **25 vulnerabilità** (per alcune delle quali ha già pubblicato dei proof of concept su GitHub) che a settembre 2019 interessavano tutte le versioni di Windows, compresa l'ultima versione di Windows 10 al tempo disponibile.

Gli sviluppatori di Redmond, spiega Dabah, hanno cominciato a lavorare sui bug già dallo scorso novembre e ne avrebbero risolti 11. Il lavoro starebbe procedendo e lo stesso ricercatore ha dichiarato di essere impegnato a sviluppare un sistema di mitigazione più ampio delle singole patch.

Condividi l'articolo

Ti presento la botnet Vollgar: 2.000 attacchi al giorno negli ultimi 2 anni

---

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/04/03/microsoft-al-lavoro-per-risolvere-25-bug-di-windows-win32k/?utm_source=rss&utm_medium=rss&utm_campaign=microsoft-al-lavoro-per-risolvere-25-bug-di-windows-win32k