Microsoft sbaglia la patch: lo zero-day è ancora una minaccia

Dic 28, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità consente di elevare i privilegi di amministrazione per avviare l'esecuzione di codice a livello kernel o creare utenti con privilegi di amministratore.

Avrebbe dovuto essere corretta a giugno, ma la patch per la vulnerabilità che affligge Windows (CVE-2020-0986) non ha ottenuto i risultati sperati.

Il bug, che interessa l'**API Print Spooler**, ha un livello di impatto piuttosto elevato (8.3 su 10) e rappresenta il classico strumento di cui i pirati informatici possono avvantaggiarsi quando riescono a introdursi nei sistemi aziendali.

Per sfruttare la vulnerabilità, è bene chiarirlo, è necessario avere già accesso a un dispositivo. Sfruttando la falla di sicurezza, però, è possibile eseguire un salto di qualità **acquisendo privilegi elevati e ottenere così una libertà d'azione maggiore rispetto a quella originale**.

Come spiegano i ricercatori di Trend Micro in un report pubblicato sul blog della società di sicurezza, la vulnerabilità è stata segnalata alla fine dell'anno scorso e, almeno in teoria, avrebbe dovuto essere corretta con l'update per Windows rilasciato lo scorso giugno.

Le cose, però, non sembrano essere andate per il verso giusto. L’aggiornamento messo a puto dagli sviluppatori di Microsoft, infatti, non ha risolto il problema e la falla di sicurezza può ancora essere sfruttata dai pirati per i loro scopi.

I ricercatori hanno contattato l’azienda per segnalare il mancato fix lo scorso settembre, assegnando **un termine di 90 giorni per risolvere il problema**. A oggi, però, dalle parti di Microsoft si sono limitati ad assegnare al bug un nuovo codice (CVE-2020-17008) prospettando il rilascio di un aggiornamento per il prossimo gennaio. Motivo per cui, i ricercatori di Trend Micro hanno reso (di nuovo) pubblica la vulnerabilità.

A questo punto, le aziende hanno un’unica soluzione: adottare politiche di mitigazione che prevedono una restrizione dei livelli di interazione con il servizio.

Condividi l’articolo

Finlandia: hacker colpiscono il parlamento Europol e Dipartimento di Giustizia USA “abbattono” tre servizi VPN

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2020/12/28/microsoft-sbaglia-la-patch-lo-zero-day-e-ancora-una-minaccia/?utm_source=rss&utm_medium=rss&utm_campaign=microsoft-sbaglia-la-patch-lo-zero-day-e-ancora-una-minaccia