SigRed: il bug in Windows Server rimasto nascosto per 17 anni

Lug 15, 2020 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

La vulnerabilità potrebbe essere sfruttata per creare un worm in grado di propagarsi autonomamente attraverso le reti locali.

Nei panni di **Microsoft**, chiunque deciderebbe di costruire un monumento a **Sagi Tzaik**. Il ricercatore di **Check Point**, infatti, è riuscito a scovare un bug di quelli che avrebbero potuto causare grossi problemi a tutte le infrastrutture IT basate su **Windows Server**.

La vulnerabilità (CVE-2020-1350) battezzata con il nome di **SigRed**, affligge Microsoft Windows DNS, il componente dedicato al **Domain Name System** dei sistemi operativi Microsoft.

Nel report pubblicato da Check Point, la vulnerabilità riguarda la possibilità che le query DNS inviate a un server provochino un buffer overflow, consentendo in pratica a un pirata informatico di eseguire codice in remoto con privilegi di sistema. **In altre parole, uno scenario da incubo che ha indotto i ricercatori ad assegnare un punteggio di 10 su 10 alla gravità di SigRed**.

[embedded content]

Il bug può essere sfruttato dall'esterno, semplicemente

attirando un utente su un sito malevolo che può provocare un crash (o l'esecuzione di codice) sul server che gestisce il DNS.

L'aggiornamento che corregge SigRed è stato distribuito da Microsoft nella tornata di update di luglio 2020 ed è quindi disponibile per chiunque. Nel loro report, però, i ricercatori di Check Point non escludono che la vulnerabilità sia già stata sfruttata in passato.

Anche perché, secondo quanto emerge dalle analisi, il codice che consente questo exploit sarebbe presente nei sistemi Windows da ben 17 anni.

Ora la vicenda è arrivata al suo "lieto fine" e si spera che gli aggiornamenti vengano eseguiti prima che qualcuno possa sfruttare SigRed per portare un attacco. SI accettano scommesse…

Condividi l'articolo

Vulnerabilità critica in SAP: 40.000 aziende a rischio per RECON

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2020/07/15/sigred-il-bug-in-windows-server-rimasto-nascosto-per-17-anni/?utm_source=rss&utm_medium=rss&utm_campaign=sigred-il-bug-in-windows-server-rimasto-nascosto-per-17-anni