Falla in ProFTPd. Un milione di server vulnerabili

Lug 23, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

Il bug permette di avviare l'esecuzione di codice in remoto. Pubblicata la patch, ma per il momento i server che l'hanno installata sono… quattro!

Si chiama **ProFTPd** ed è uno di quei componenti che probabilmente non abbiamo mai sentito nominare. Si tratta di un server FTP cross-platform che supporta sia i sistemi basati su Unix, sia Windows. Il software, però, contiene una falla di sicurezza (CVE-2019-12815) che apre la strada ad attacchi in remoto.

Come spiega **Tobias Mädel**, il ricercatore che ha individuato la vulnerabilità, il problema riguarda il modulo **mod_copy**, che nelle installazioni di ProFTPd è attivato come impostazione predefinita.

Il bug, che rappresenta una variante di una vulnerabilità del 2015, consentirebbe di usare i comandi *SITE CPFR* e *SITE CPTO* per eseguire operazioni di lettura e scrittura sui server vulnerabili aggirando i sistemi di autenticazione. In pratica, spiega Mädel, è possibile copiare qualsiasi file in remoto sui server.

Eseguendo una ricerca su **Shodan** (il servizio online che permette di individuare qualsiasi dispositivo o processo su Internet) risultano più di un milione di server con ProFTPd attivo.

La maggior parte di questi sarebbe vulnerabile a un eventuale attacco. La vulnerabilità, infatti, non interessa la versione **1.3.6** del componente, pubblicata il 17 luglio scorso. **Peccato che, sempre su Shodan, i server con la versione aggiornata siano soltanto quattro**.

Non è detto però che tutti i server non aggiornati siano vulnerabili. **Come spiegano i ricercatori, per eliminare il rischio di un attacco è sufficiente disabilitare il modulo mod_copy**. Accettiamo scommesse su quanti amministratori lo abbiano fatto.

Condividi l’articolo

Come funziona la smart home e come è possibile hackerarla!

Articoli correlati

Altro in questa categoria

---

https://www.securityinfo.it/2019/07/23/falla-in-proftpd-un-milione-di-server-vulnerabili/