Google rende pubblica una falla zero-day nei router TP-Link

Mar 29, 2019 Marco Schiaffino In evidenza, News, RSS, Scenario, Vulnerabilità 0

Ennesimo sgarbo del Project Zero di Google: TP-Link non ha pubblicato l'aggiornamento entro i termini imposti dai ricercatori. Ora i pirati possono fare festa.

È una vulnerabilità di quelle che fanno venire i brividi e che consentirebbe a un pirata informatico di avviare l'esecuzione arbitraria di codice su un router attraverso la rete locale.

A soffrirne sono i router **TP-Link SR20 Smart Home** a causa di un processo chiamato **tddp (TP-Link Device Debug Protocol)** e che consente di inviare dei comandi al dispositivo.

La funzionalità, nel dettaglio, prevede la possibilità di inviare due tipi di comandi: il primo non richiede l'autenticazione come amministratore, il secondo invece sì.

Il problema è che uno dei comandi del primo tipo (**command 0x1f, request 0x01**) consente di inviare richieste tramite il **Trivial File Transfer Protocol (TFTP)**, che vengono elaborate da un interpreter con privilegi di root. Risultato: è possibile inviare qualsiasi tipo di comando al sistema, prendendo di fatto il controllo del dispositivo.

La vulnerabilità è stata individuata dal solito **Project Zero di Google**, che dopo averla comunicata a TP-Link ha concesso i canonici **90 giorni** all'azienda per sviluppare e distribuire la patch che la corregge. **Passata la scadenza, Matthew Garrett**

(il ricercatore di Google che ha individuato la falla) ha reso pubblica la falla zero-day.

Non solo: giusto per rendere le cose più semplici ai pirati informatici che volessero sfruttarla, lo stesso Garrett ha pubblicato un Proof of Concept che permette di sfruttare l'exploit.

Non è la prima volta che il Project Zero pubblica i dettagli di vulnerabilità zero-day in seguito al mancato rispetto da parte dei produttori delle rigide scadenze integrate nella loro policy di "responsible disclosure".

La vittima preferita di Google, in questo senso è **Microsoft**, che ha visto pubblicare vulnerabilità relative ai suoi prodotti nel febbraio 2017 e nel febbraio 2018.

Anche se la previsione di deadline è uno strumento utile per vincere l'inerzia dei produttori nello sviluppo delle patch, una cosa è certa: i ricercatori del Project Zero non hanno molte chance di vincere il **premio simpatia** da parte dei colleghi.

Please follow and like us:

Cisco corregge 27 bug, ma due router rimangono vulnerabili

Articoli correlati

Altro in questa categoria

https://www.securityinfo.it/2019/03/29/google-rende-pubblica-una-falla-zero-day-nei-router-tp-link/