

Nuove falle nel controllo remoto di Windows: aggiornare!

Ago 14, 2019 Marco Schiaffino In evidenza, News, RSS, Vulnerabilità 0

L'ultimo update di Microsoft corregge quattro vulnerabilità nel Remote Desktop Service che consentono attacchi in remoto senza autenticazione.

Dopo aver corretto in fretta e furia **Bluekeep**, la vulnerabilità che consentiva di violare un sistema Windows attraverso un collegamento in remoto che non richiede alcuna interazione da parte dell'utente, Microsoft si trova a fronteggiare altre quattro (quattro!) falle di sicurezza con le stesse caratteristiche.

L'anello debole, ancora una volta, è quel **Remote Desktop Service** che le aziende trovano terribilmente utile per gestire a distanza i loro computer ma che si sta dimostrando anche incredibilmente fragile sotto li profilo della sicurezza.

Questa volta le vulnerabilità sono state scoperte dal team di sicurezza interno di Microsoft. I bug (CVE-2019-1181, CVE-2019-1182, CVE-2019-1222 e CVE-2019-1226) interessano tutte le versioni del sistema operativo: **Windows 7, Windows 8.1, Windows Server 2008, Windows Server 2012 e Windows 10.**

La descrizione delle vulnerabilità, piuttosto stringata, è uguale per tutte: sfruttandole un pirata informatico potrebbe ottenere il controllo completo di un computer semplicemente inviando dei pacchetti attraverso il **Remote Desktop Protocol**.

Niente autenticazione e nessuna necessità di ingannare l'utente per fargli fare clic su un collegamento o aprire un file. **Insomma: saremmo di fronte a un classico exploit che permetterebbe ai cyber-criminali di creare un worm in grado di diffondersi autonomamente.**

Le falle di sicurezza sono state corrette nell'ultimo aggiornamento per i sistemi Windows e si spera, di conseguenza, che il pericolo sia scampato.

Per tutti quelli che non potessero applicare le patch (non si capisce bene per quale motivo, ma ce ne sono ancora) l'alternativa è quella di disabilitare il servizio di controllo remoto o inserire un blocco da firewall sulla porta TCP 3389.

La buona notizia è che, fino a ora, non è comparso alcun exploit in grado di sfruttare le vulnerabilità. Dal punto di vista dei pirati, quindi, si è all'anno zero.

Condividi l'articolo

Quattro app per appuntamenti rivelano l'esatta posizione degli

utenti Router 4G a rischio attacco. Avete aggiornato il firmware?

Articoli correlati

Altro in questa categoria

<https://www.securityinfo.it/2019/08/14/nuove-falle-nel-controllo-remoto-di-windows-aggiornare/>