

## TFTP

Recentemente Sunrise potrebbe averle inviato una lettera e/o un'e-mail nella quale le ha segnalato di aver ricevuto una notifica relativa a un dispositivo nella sua rete che presenta una vulnerabilità nota come TFTP aperto. Se ha ricevuto tale comunicazione, la preghiamo di seguire le istruzioni fornite su questa pagina per risolvere il problema.

### Panoramica

TFTP è un servizio che consente ad altri dispositivi di una rete di accedere da remoto a file e cartelle su un dispositivo che esegue il servizio senza dover utilizzare le credenziali di accesso. Questo servizio è progettato solo per l'utilizzo su una piccola rete locale, come ad esempio la sua abitazione, ma se esposto a Internet nel senso più ampio può essere utilizzato abusivamente da terzi.

### Cosa è accaduto?

Collaboriamo con diverse organizzazioni senza scopo di lucro di diversi settori della sicurezza che raccolgono informazioni su Internet relative ai dispositivi che sembrerebbero essere compromessi o configurati in modo errato. Ciò significa che il suo dispositivo compromesso o configurato in modo errato è accessibile a chiunque su Internet e che la scansione effettuata da queste organizzazioni non rientra nella sua rete privata.

Sospettiamo che un dispositivo collegato alla sua rete domestica presenti una vulnerabilità del TFTP aperto. Per maggiori informazioni su questi rapporti visiti [tftpscan.shadowserver.org](https://tftpscan.shadowserver.org)

Se viene lasciato libero accesso alle impostazioni, queste possono essere sfruttate per rubare dati personali e partecipare inconsapevolmente ad attività dannose, come ad esempio un attacco Distributed Denial of Service (DDoS).

Ecco perché è importante che segua i consigli di questo articolo.

Nota: lo scopo di questo articolo è fornirle alcuni suggerimenti. Sunrise non è responsabile di eventuali inconvenienti occorsi durante la risoluzione del problema e non è in grado di fornire supporto tecnico per tali questioni.

### Come si può risolvere il problema?

È possibile risolvere una vulnerabilità del TFTP aperto impostando il firewall per bloccare la porta UDP 69.

Si prega di notare che il blocco di questa porta impedirà solo il traffico in uscita o in entrata attraverso questa porta verso la/dalla sua rete domestica. I servizi all'interno della sua abitazione che utilizzano tale porta dovrebbero continuare a funzionare normalmente.

Per rendere inaccessibile la porta vulnerabile:

- Acceda alla pagina di configurazione del suo router
- Acceda con il suo nome utente e password. Di default vengono visualizzati sul router stesso
- Selezioni l'opzione Port Forwarding
- Rimuova qualsiasi regola che lasci aperta la porta 69
- Selezioni l'opzione Port Trigger
- Rimuova qualsiasi regola che lasci aperta la porta 69

Si assicuri che tutti i dispositivi nella sua rete siano protetti da un firewall. È importante verificare che tutti i suoi dispositivi siano coperti dalla protezione di un firewall.

### Questioni relative a Internet

Sunrise è co-fondatrice e membro di iBarry.ch, un'organizzazione senza scopo di lucro che collabora con esperti di sicurezza online per fornirle tutte le informazioni necessarie volte a proteggere lei e i suoi bambini online.

Ulteriori informazioni su iBarry sono disponibili su <https://www.ibarry.ch/it/>