A TLC srl
Via 1° Maggio, 26 / 60131 Ancona (Italy)
Tel. +39 071 250651 / Fax +39 071 2506518
www.aethra.com - info@aethra.com

Servizio SSH port forwarding

Gentile Cliente,

Si segnala che l'implementazione del server SSH su Release ATOS NT 5.5.x e 5.6.x fino alla versione 5.6.18 presenta la funzionalità di SSH local port forwarding attiva. Essa consente l'apertura di una sessione ssh con local port forwarding configurabile sul client che si connette alla CPE dalla Wan, ad esempio verso un web server, lasciando in sospeso l'autenticazione alla CLI. Da quel momento è possibile effettuare traffico sul "tunnel" configurato da un client SSH, dando quindi la possibilità accedere ad un servizio in rete con l'IP sorgente del CPE con server SSH senza essere a conoscenza di credenziali del CPE.

Per quanto sopra descritto il CPE potrebbe essere utilizzato in modo improprio per effettuare spoofing attacks (in particolare su rete Internet).

Dalla versione ATOS NT 5.6.19 in avanti la funzionalità sopra descritta è stata disabilitata.

Nel caso di utilizzo di versioni ATOS NT con funzionalità di SSH local port forwarding attiva, si suggeriscono una delle seguenti contromisure:

1. Disabilitare il servizio SSH, se non utilizzato per il management della CPE, con il comando “set system intservices ssh 0”
2. Utilizzare un’accesslist che permetta l’accesso al servizio SSH solo da reti “consentite”

Si ribadisce inoltre che dalla release ATOS NT 5.6.19 o superiori la funzionalità sopra descritta è stata disabilitata.

Aethra Telecommunications resta a disposizione per qualsiasi chiarimento e supporto.

Luca Messina
CTO/CMO
Aethra Telecommunications
A TLC S.R.L.

Ancona 28/01/2015

SSH port forwarding Service

Dear Customer,

SSH server implementation in ATOS NT Release 5.5.x and 5.6.x (up to version 5.5.18) has SSH local port forwarding active.

This feature allows to open a ssh session with local port forwarding enabled (i.e. towards a Web Server) configurable in the Client connected to the CPE from the WAN, leaving the CLI authentication pending. From that point it is possible to make traffic in the configured “tunnel” from a SSH Client, giving the possibility to access a network service using the CPE IP address as source.

Because of this the CPE could improperly be used for spoofing attacks (mainly in Internet).

Starting from ATOS NT 5.6.19 on the above feature has been disabled.

With previous versions it is strongly suggested to use one of the following settings:

1. Disable the SSH service if not used for management purposes, using the command “set system intservices ssh 0”;
2. Configure an accesslist that allows the access through SSH only from “trusted networks”

We remind that from firmware release 5.6.19 the above feature has been disabled.

Aethra Telecommunications is available for any clarification and support request.

Luca Messina
CTO/CMO
Aethra Telecommunications
A TLC S.R.L.

Ancona 28/01/2015