Vulnerability detection on TP-Link routers allows an attacker to log in without a password

A serious security flaw affects some Archer routers, which could allow potential attackers to control devices over a remote LAN via a Telnet connection without having to provide confidentiality. administrator password.

TP-Link has just announced the successful development of a patch for a serious security hole affecting some Archer routers, which could allow potential attackers to control devices through Remote LAN via Telnet connection without having to provide administrator password.

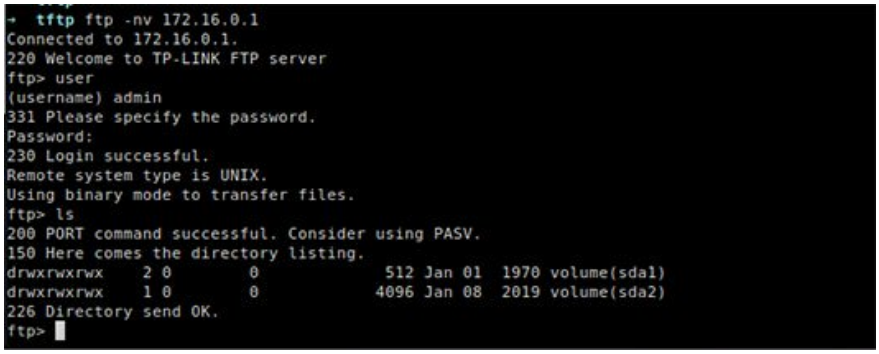
'In the case of a successful exploit, this vulnerability could allow a remote attacker to control the configuration of the router via Telnet on the local area network (LAN) and connect to the FTP server via LAN or WAN ', said security expert Grzegorz Wypych of the IBM X-Force Red team.

To exploit this security vulnerability, an attacker must send an HTTP request that contains a string longer than the number of bytes allowed, resulting in the user password being completely disabled and replaced with a value. hollow.

The built-in authentication is completely 'useless' in this case because it only checks the referrer's HTTP headers, allowing the attacker to mislead the httpd router service that this request is valid by Use hard-coded tplinkwifi.net value.

The users of these routers are mainly system administrators, who have full root access, so once the threat actors can bypass the authentication process, they will automatically gain administrative privileges. administrator on the router. After that, all processes will be run by this access holder. As such, it can be said that the attacker acted as an administrator and successfully hijacked the device.

"Attackers not only can gain high-level access, but legitimate users will also be blocked and no longer be able to log in to the web service through the regular user interface, resulting in no unable to reset new password ', added Mr. Grzegorz Wypych.



Worse, even if the router owner sets a new password, an attacker can continue to disable it with a LAN / WAN / CGI request, causing the USB connection to the built-in FTP server to become The only way to access the router. In addition, RSA encryption keys will not be applicable in this case because they do not work with blank passwords.

This vulnerability is being monitored with the identifier CVE-2019-7405, affecting Archer C5 V4, Archer MR200v4, Archer MR6400v4 and Archer MR400v3 routers. TP-Link has released patches to help customers protect their routers from related attacks. As follows:

TP-Link routers are affected by Archer C5 V4 security patch https://static.tp-link.com/2019/201909/20190917/Archer_C5v4190815.rarArcher MR200v4https://static.tp-link.com/2019/201909/20190903/Archer%20MR200(EU)_V4_20190730.zipArcher MR6400v4https://static.tp-link.com/2019/201908/20190826/Archer%20MR6400(EU)_V4_20190730.zipArcher MR400v3https://static.tp-link.com/2019/201908/20190826/Archer % 20MR400 (EU) _V3_20190730.zip