Vulnerability affecting TP-Link Routers

Introduction

It was recently discovered that some common routers from multiple manufacturers are affected by a vulnerability that under some circumstances could allow manufacturers to obtain the administrative password for said router.Cerberus has checked the routers that we have supplied in the last 6 years and we have identified 1 model of router which are affected by this issue. This is:

- TP-Link W8951ND V5

For avoidance of doubt the other routers that we have supplied, such as other TP-Link (including earlier versions V1, V3 & V4 of the W8951ND), Thomson, Cisco & Draytek , are not believed to have this vulnerability.

The Risk

The vulnerability allows an attacker to target the router using a special URL. This URL allows them to download a backup of the routers configuration. Although this backup file is encoded there has been made available a tool which allows the attacked to reverse engineer the Administrator password.

By default as the routers ship from the factory remote access to the routers is disabled. With remote access disabled it is not possible to attack the router from the Internet, it could only be attacked from the customers own LAN which is relatively unlikely. If remote access has been enabled then if you have configured an ACL (access control list) then again the router cannot be attacked from the Internet at large.

If you have remote access enabled to the Internet, and have no ACL in force then your router is vulnerable. We have seen an attack which exploits this vulnerability by changing the DNS servers on customer equipment and potentially redirecting attackers to fake versions of popular website. As soon as this was discovered we made changes to our network to block the IP addresses used by these attackers.

If you are already using the latest firmware (140226 or 140306) then you are not susceptible to this vulnerability.

Our Recommendation

If you or your customer uses the model of router affected, then we suggest that you upgrade your firmware to the latest version. The latest version corrects this vulnerability. Software and Instructions to do this can be found here:

1. http://www.tp-link.com/en/support/download/?model=TD-W8951ND&version=V5
2. Check the configuration of the router for suspicious DNS servers. If in doubt change the name servers to those provided for Cerberus Customers: 46.37.32.22 & 46.37.33.22.
3. Change the administrator password on the router.
4. (Optional if upgrading firmware) Setup an ACL to limit remote access to only IP addresses from which you expect to remotely manage your equipment.

If you cannot carry out these all steps immediately, for instance you may be unhappy carrying out a firmware upgrade from remote, then we recommend that you still carry out steps 2 through 4 above. If you do not upgrade the firmware then the router will still be vulnerable from the LAN side, but not from the Internet as a whole.

Cerberus End User Customers

If we maintain a customer's router and we believe it to be vulnerable then we will attempt to connect to the router remotely and take the steps above. This work would be carried out overnight.

Frequently Asked Questions

Q. I know that I have a W8951ND, but I do not know if it is the V5. What should I do?

A: If you have physical access to the router the easiest way is to look at the sticker on the underside of the router as described here: http://www.tp-link.com/en/article/?faqid=46

If you only have remote access then look at the current firmware version which will show either 5.0.0 Build 120522 Rel.23978 or 5.0.0 Build 131104 Rel. 09041 If you have version 5 hardware and are affected.

Q. How can I tell if I have an ACL configured?

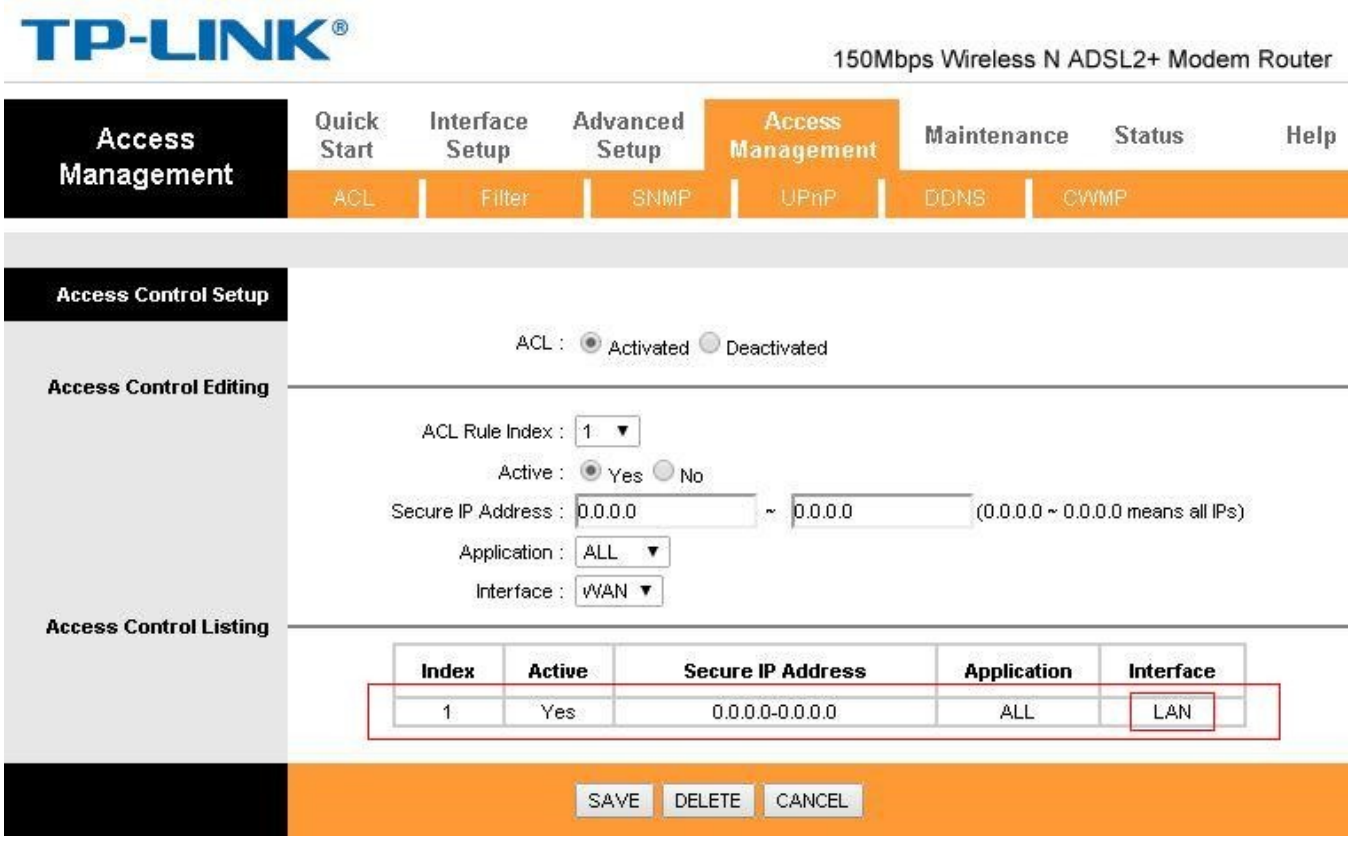
A:

a. Please log into the management webpage of your modem router, and go to Access Management -> ACL.

b. By default, the configurations should be just like the following picture shows (the value of the **Interface** setting is **LAN**). You just need to make sure your modem router's configurations are exactly the same.

c. If you don't know how to configure ACL on your modem router, please click this link

http://www.tp-link.com/en/article/?faqid=476


TP-LINK®
150Mbps Wireless N ADSL2+ Modem Router
Access Management
Quick Start
Interface Setup
Advanced Setup
Access Management
Maintenance
Status
Help
ACL
Filter
SNMP
UPnP
DDNS
CWMP
Access Control Setup
ACL : Activated Deactivated
Access Control Editing
ACL Rule Index : 1
Active : Yes No
Secure IP Address : 0.0.0.0 ~ 0.0.0.0 (0.0.0.0 ~ 0.0.0.0 means all IPs)
Application : ALL
Interface : WAN
Access Control Listing
Index
Active
Secure IP Address
Application
Interface
1
Yes
0.0.0.0-0.0.0.0
ALL
LAN
SAVE
DELETE
CANCEL