Critical Misconfiguration in the Firewall Rules of ACT's Customer Intranet

Sujal Singh
contact@sujal.dev

Abstract

This report details a critical misconfiguration in the firewall rules of the local network of customers created by ACT Fibernet to share a single public IPv4 address with multiple customers behind a CGNAT. There exists no rule that blocks communication between two clients connected to this network. This is currently allowing customers belonging to a particular network to access each other's devices.

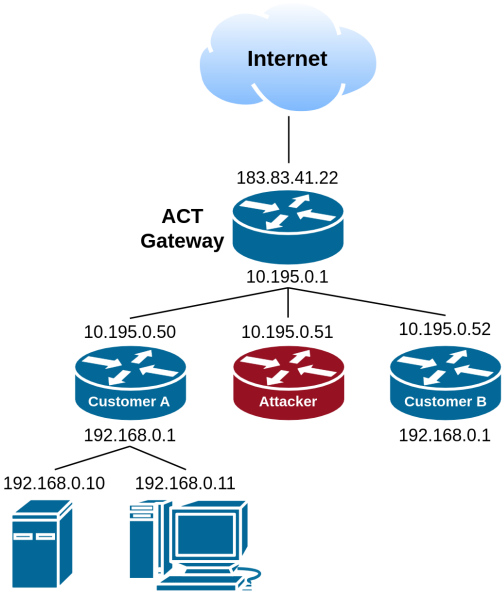

Figure 1: Customer Intranet

A malicious customer can gain access to any device on the network with a default password, or exploit any other vulnerability present in the device to gain access. Some routers distributed by ACT also have a default password of *"act@123"*. Once an attacker gains access to a device such as the router, it will have control over the entire network of the target, allowing the attacker to carry out **several high severity attacks** such as DNS hijacking. All of this is easily preventable if ACT takes the necessary steps to fix the issue.

1. Steps to reproduce

A malicious customer can use any network scanner such as *nmap* to perform network discovery. But first one has to figure out a few parameters to begin scanning the network.

1. Figure out your gateway's gateway, i.e, the gateway of the local network created by ACT. This can be done by running the following command (on a *nix machine):

   ```
   $ traceroute example.com
   ...
    2  10.195.0.1 (10.195.0.1)  4.526 ms  4.690 ms
   ...
   ```

   This is usually going to be the second hop in the output, in this case it's `10.195.0.1`. This assumes that there exists a router between you and ACT's router and you're not directly plugging in the WAN cable coming to your home to the device you're using to run traceroute.

2. One can now begin scanning the network by running the following (change the IP address according to the value received in the previous step):

   ```
   $ nmap -p 80 10.195.0.0-255
   ```

   In this example, I've chosen to only scan a small portion of the network with devices that have port 80 open so that the scan is fairly quick. A full network scan would take a very long time.

3. Once the network scan is complete, visit each host that has port 80 open in a web browser (keep in mind that port 80 doesn't necessarily imply an http server) and one will encounter router management portals, CCTV cameras (some cameras have particular ports open, identifying those and running the scan to look for only those ports can quickly find many open cameras of the same build which likely have the same default password), NAS devices, printers, etc.

2. Proof of Concept

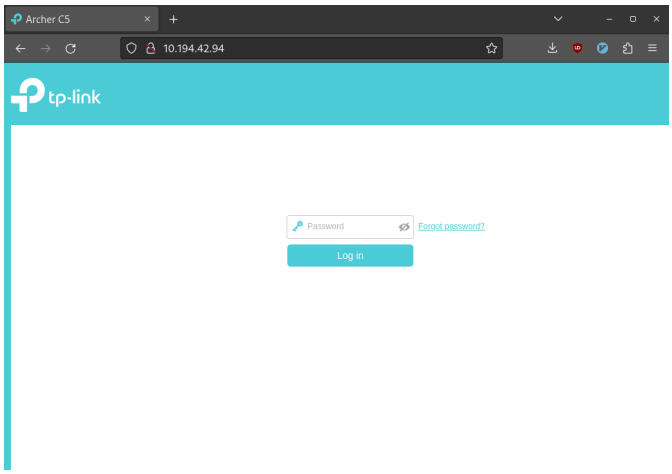

Figure 2: TP Link router with common default passwords

Figure 3: MikroTik router

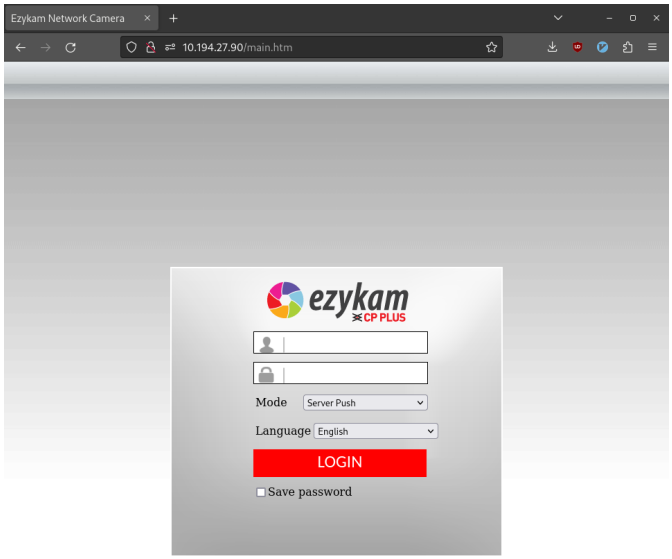

Figure 4: CP Plus CCTV with common default passwords

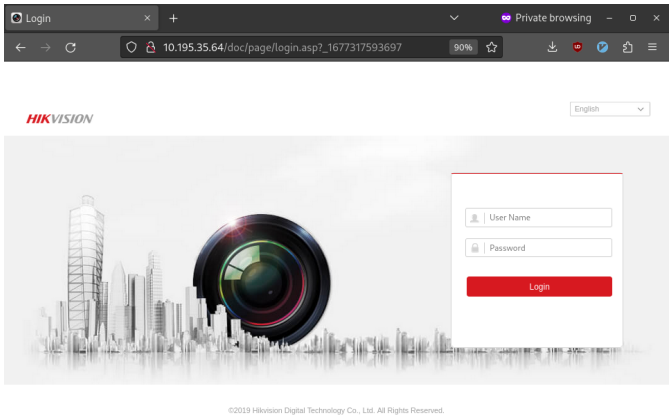

Figure 5: HikVision CCTV

Note: there exist many more examples in the attached documents.

3. Impact

The lack of existence of a firewall rule blocking inter-customer communication exposes ACT's customers to innumerable critical attacks. The severity of threats vary with the type of device compromised by the attacker. The

following are only some of the potential threats that arise as a result of exposing devices on a customer intranet of this type.

3.1 Routers

An attacker will easily be able to access routers with default passwords, giving the attacker various information such as the WiFI password and SSID, hostnames of the hosts connected to the LAN, etc.

3.1.1 DNS Hijacking

An attacker can configure a malicious DNS server to be advertised via DHCP on the target's router, allowing it to direct any domain to any IP address. The attacker could also simply just monitor which sites a user visits, which violates the privacy of the target.

3.1.2 Phishing

Having control over the DNS server will allow the attacker to employ phishing attacks on the target, including but not limited to **net banking sites, email, other such critical services.**

3.1.3 Fake CA Certificate

Once the attacker has configured a malicious DNS servers it can redirect the target to a fake warning page which employs various social engineering techniques to manipulate the user into installing a CA certificate owned by the attacker.

3.1.4 Man in the Middle

Having control over the DNS server and having a fake CA certificate installed on the target's machine, the attacker can now MITM all traffic, including encrypted traffic. The possibilities here are endless.

3.1.5 PPPoE Credentials

The attacker might be able to figure out the **name, email, mobile number, address** of the target. The attacker can obtain the PPPoE credentials of the target by accessing the target's router. Feeding bogus PPPoE credentials to target's router so that there is no conflict for the next step. Visiting selfcare.actcorp.in and logging in with the obtained credentials will reveal the aforementioned information.

3.1.6 Port Forwarding

The attacker can setup port forwarding rules to any device such as a printer, CCTV camera, smart door locks, computers, etc. on the target's network. Being able to control a smart lock remotely is particularly dangerous.

3.1.7 DDoS

The attacker can employ various combinations of the above points to compromise an entire fleet of devices, creating a botnet. The botnet can be used for various malicious purposes including a DDoS attack originating from the IP addresses registered under ACT's name which has the potential to damage ACT's reputation globally depending on the target of the DDoS attack.

3.2 CCTV Cameras

An attacker can gain access to CCTV cameras having default passwords (which is fairly common) connected to the network. One can monitor, control, disable the camera without the target having any idea. Needles to say this is a giant breach into the target's privacy and could also have real world consequences, such as disabling a camera during a robbery.

4. Proposed Solution

The solution to this problem is fairly straightforward. ACT Fibernet could setup a firewall rule that blocks any customer-to-customer communication on that network since it does not serve any purpose and exposes the network to a plethora of attacks. Even if two clients need to communicate with each other on this intranet for whatever reason, a simple exception rule could be setup after assigning both of those clients a private static IP or setup an entire block of IP addresses to allow such communication.