Persistant Backdoor Process

The following outlines the procedure to create a persistent backdoor. First, the authentication logic prepends a salt to the plaintext password stored on the router in the password authentication phase. It then echos that combined string to md5sum via a *shell command*.
The shell command is roughly equivalent to:

```
system("echo -n '%s' | md5sum")
```

where the *%s* would be replaced with the salt/password combo.

Since we have already gained access through other RCE mechanisms, we can set the password on the router without going through the web UI, which disallows spaces and certain special characters. Instead, we run a *nvram_set* command, which is symlinked to the *ralink_init* binary, by running the following code:

```
nvram_set 2860 Password NewPassword123
```

We can set the password to a shell injection such that the final command looks something like:

```
system("echo -n '<salt>'<shell command>'' | md5sum")
```

Furthermore, we can have the shell command echo the user's original password. Thus regular web authentication will appear normal to the user. The command functionally becomes:

```
system("echo -n 'saltpassword' | md5sum")
```

Note: *password changing makes a strict comparison between the plaintext passwords, so the user would be unable to change their password.*

Since the NVRAM on this device persists through reboots and firmware updates, the shell injection gets triggered on boot. While we cannot precisely determine which program starts it, we think it is the */bin/web* binary. That binary uses the plaintext password from NVRAM and has similar constructs with shell commands to get md5 digests.

Each time a user tries to log into the web interface, this injection is triggered. This behavior provides an attacker a method to restart their (bind/reverse) shell on-demand. For CVE-2020-13117, this is the alleged exploitation location. However, after finding that CVE, we tried to replicate the shell injection through the salt via the web interface and were unable, as there now appears to be some filtering for single quotes.