

Monospace Directus Headless CMS File Upload / Rule Bypass

Authored by [Moritz Friedmann](#), [Oliver Boehlk](#) | Site [sec-consult.com](#)

Posted Apr 7, 2021

Monospace Directus Headless CMS versions prior to 8.8.2 suffers from .htaccess rule bypass and arbitrary file upload vulnerabilities.

tags | [exploit](#), [arbitrary](#), [vulnerability](#), [file upload](#)
advisories | [CVE-2021-29641](#)

SHA-256 | 0a87fe85b52203eaf5e6bafacaf4a67e5b5538421123168457d798bfb86748dd [Download](#) | [Favorite](#) | [View](#)

Related Files

Share This

Like

Twitter

LinkedIn

Reddit

Digg

StumbleUpon

[Change Mirror](#)[Download](#)

SEC Consult Vulnerability Lab Security Advisory < 20210407-0 >

title: Arbitrary File Upload and Bypassing .htaccess Rules
product: Monospace Directus Headless CMS
vulnerable version: < v8.8.2
fixed version: v8.8.2, v9 is not affected because of different architecture
CVE number: CVE-2021-29641
impact: High
homepage: <https://directus.io/>
found: 2020-12-15
by: Oliver Boehlk (AtoS Germany)
Moritz Friedmann (AtoS Germany)
SEC Consult Vulnerability Lab

An integrated part of SEC Consult, an AtoS company
Europe | Asia | North America

<https://www.sec-consult.com>

Vendor description:

"Directus Open-Source, Free & Unlimited. No Strings Attached.
Our premium software is available at no cost for commercial and personal use.
This self-hosted version is full-featured, with no artificial limitations."
Source: <https://directus.io/open-source/>

Business recommendation:

The vendor provides an updated version for v8 which fixes the security issue. It should be installed immediately.

Note: Directus v8 has been deprecated/discontinued and is replaced by version 9, which currently does not have a final release version yet. Updating to Directus v9 fixes this vulnerability as well because the NodeJS architecture replaces the PHP API and hence is not affected.

According to the vendor, the identified security issue only applies to v8 installations relying on the specific Apache-based config in the Docker image, using the local-storage driver for uploads. The recommendation from the vendor is to use a connection to S3 for such installations, install the patch v8.8.2 or upgrade to version 9.

Vulnerability overview/description:

1) Arbitrary File Upload and Bypassing .htaccess Rules (CVE-2021-29641)
Any low privileged user with file upload permissions can upload webshells or other malicious PHP files which can be found in /uploads/_/originals/.

If the server prevents the execution of PHP files in the upload directory the attacker can move the file into a subdirectory where he can upload a custom .htaccess file to enable PHP execution again.

Server side command execution can be used to retrieve the Directus configuration and database credentials to escalate in-app privileges, retrieve password hashes or move laterally in the network.

Proof of concept:

1) Arbitrary File Upload and Bypassing .htaccess Rules (CVE-2021-29641)
A PoC environment can be created using a docker-compose.yml file:

version: "3"

services:
 app:
 image: directus/directus:v8.8.1-apache
 ports:
 - 8080:80
 environment:
 DIRECTUS_INSTALL_TITLE: vulnerable directus server
 DIRECTUS_INSTALL_EMAIL: admin@ha.ck
 DIRECTUS_INSTALL_PASSWORD: admin1
 DIRECTUS_AUTH_SECRETKEY: directusprivtest
 DIRECTUS_AUTH_PUBLICKEY: directuspubtest
 DIRECTUS_DATABASE_HOST: db
 DIRECTUS_DATABASE_NAME: directus
 DIRECTUS_DATABASE_USERNAME: directus
 DIRECTUS_DATABASE_PASSWORD: directus
 db:
 image: mariadb
 environment:
 MYSQL_ROOT_PASSWORD: directusr00t
 MYSQL_DATABASE: directus
 MYSQL_USER: directus
 MYSQL_PASSWORD: directus

Optionally, Directus data folders can be mounted for persistent storage:
volumes:
 - ./data/config:/var/directus/config
 - ./data/uploads:/var/directus/public/uploads

An .htaccess file can be placed in the uploads directory to prevent PHP execution:
<#Module mod_php7.c>
 php_flag engine off
</#Module>

Initial installation requires "install" to be called:
docker-compose up -d && docker-compose run app install

Login defined in docker-compose:
admin@ha.ck:admin1

An attacker can upload a PHP file and open it at uploads/_/originals/[randomid].php.
If a .htaccess file is used, the code does not get executed and gets returned in plain text.

You can edit the item in Directus and change the Filename Disk to "test/file.php" (it doesn't matter that there is no folder named test yet, Directus/Apache does you a favor and creates it

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 157 files
Ubuntu 76 files
LiquidWorm 23 files
Debian 21 files
nu11security 11 files
malvuln 11 files
Gentoo 9 files
Google Security Research 8 files
Julien Ahrens 4 files
T. Weber 4 files

File Tags

ActiveX (932)	December 2022
Advisory (79,754)	November 2022
Arbitrary (15,694)	October 2022
BBS (2,859)	September 2022
Bypass (1,619)	August 2022
CGI (1,018)	July 2022
Code Execution (8,926)	June 2022
Conference (673)	May 2022
Cracker (840)	April 2022
CSRF (3,290)	March 2022
DoS (22,602)	February 2022
Encryption (2,349)	January 2022
Exploit (50,359)	Older
File Inclusion (4,165)	

File Upload (946) Systems

Firewall (821)	AIX (426)
Info Disclosure (2,660)	Apple (1,926)
Intrusion Detection (867)	BSD (370)
Java (2,899)	CentOS (55)
JavaScript (821)	Cisco (1,917)
Kernel (6,291)	Debian (6,634)
Local (14,201)	Fedora (1,690)
Magazine (586)	FreeBSD (1,242)
Overflow (12,419)	Gentoo (4,272)
Perl (1,418)	HPUX (878)
PHP (5,093)	iOS (330)
Proof of Concept (2,291)	iPhone (108)
Protocol (3,435)	IRIX (220)
Python (1,467)	Juniper (67)
Remote (30,044)	Linux (44,315)
Root (3,504)	Mac OS X (684)
Ruby (594)	Mandriva (3,105)
Scanner (1,631)	NetBSD (255)
Security Tool (7,777)	OpenBSD (479)
Shell (3,103)	RedHat (12,469)
Shellcode (1,204)	Slackware (941)
Sniffer (886)	Solaris (1,607)

for you).

Now you can access the file at /uploads/_originals/test/file.php.
Even if you delete the file in Directus it remains on the server, and can be accessed via the above mentioned URL.

To get code execution the next step is to simply upload an own .htaccess file containing

```
<IfModule mod_php7.c>
    php_flag engine on
</IfModule>
```

And again change the Filename Disk to test/.htaccess.

Now calling /uploads/_originals/test/file.php executes the PHP file.

Vulnerable / tested versions:

The following versions have been tested and found to be vulnerable. According to the vendor, only the Apache-based docker image with the local-storage driver is affected and not the Directus suite as a whole.

```
* v8.4.0
* v8.8.1 (latest version at the time of the test)
```

It is assumed that all previous v8 versions are affected as well.

Version 9 uses a different architecture and is not affected by this vulnerability.

Vendor contact timeline:

2020-12-16 | Contacting vendor through security@directus.io; no reply
2021-03-04 | Contacting vendor again through security@directus.io
2021-03-05 | Vendor reply, exchanged S/MIME certificates
2021-03-08 | Sending security advisory to vendor
2021-03-12 | Asking the vendor whether they received the advisory; no reply
2021-03-25 | Asking vendor again for status update
2021-03-25 | Vendor: v8 will be fixed in new version
2021-03-26 | Vendor: the issue has been fixed in v8.8.2 available at dockerhub
2021-04-07 | Coordinated release of security advisory

Solution:

The vendor provides an updated version v8.8.2 at dockerhub which fixes the security issue:
<https://hub.docker.com/layers/directus/directus/v8.8.2-apache/images/sha256-d9898b642b0150c3c377b50e706757f35d2d563bd82daf97f3ae4ba450a6e67context=explore>

Alternatively, version 9 can be installed as well, which uses a different architecture and is not affected.

Workaround:

None

Advisory URL:

<https://sec-consult.com/vulnerability-lab/>

SEC Consult Vulnerability Lab

SEC Consult, an Atos company
Europe | Asia | North America

About SEC Consult Vulnerability Lab
The SEC Consult Vulnerability Lab is an integrated part of SEC Consult, an Atos company. It ensures the continued knowledge gain of SEC Consult in the field of network and application security to stay ahead of the attacker. The SEC Consult Vulnerability Lab supports high-quality penetration testing and the evaluation of new offensive and defensive technologies for our customers. Hence our customers obtain the most current information about vulnerabilities and valid recommendation about the risk profile of new technologies.

Interested to work with the experts of SEC Consult?
Send us your application <https://sec-consult.com/career/>

Interested in improving your cyber security with the experts of SEC Consult?
Contact our local offices <https://sec-consult.com/contact/>

Mail: research@sec-consult.com
Web: <https://www.sec-consult.com>
Blog: <http://blog.sec-consult.com>
Twitter: https://twitter.com/sec_consult

EOF O. Boehlk, M. Friedmann / #2021

Spoof (2,166)	SUSE (1,444)
SQL Injection (16,102)	Ubuntu (8,199)
TCP (2,379)	UNIX (9,159)
Trojan (686)	UnixWare (185)
UDP (876)	Windows (6,511)
Virus (662)	Other
Vulnerability (31,136)	
Web (9,365)	
Whitepaper (3,729)	
x86 (946)	
XSS (17,494)	
Other	

[Login](#) or [Register](#) to add favorites

packet storm
© 2022 Packet Storm. All rights reserved.

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