SEC Consult SA-20210407-0 :: Arbitrary File Upload and Bypassing .htaccess Rules in Monospace Directus Headless CMS

From: SEC Consult Vulnerability Lab <research () sec-consult com>
Date: Wed, 7 Apr 2021 12:12:02 +0200

```
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: directusroot
      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:
<IfModule mod_php7.c>
  php_flag engine off
</IfModule>


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
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-
d9898b6442b0150c3c377b50e706757f35d2d563bd82ddaf97f3ae4ba450a6e6?context=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 at sec-consult dot 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
```

Attachment: `smime.p7s`
Description: S/MIME Cryptographic Signature

By Date By Thread

Current thread:

SEC Consult SA-20210407-0 :: Arbitrary File Upload and Bypassing .htaccess Rules in Monospace Directus Headless CMS *SEC Consult Vulnerability Lab (Apr 07)*

Site Search

Nmap Security Scanner
Ref Guide

Npcap packet capture
User's Guide

Security Lists
Nmap Announce
Nmap Dev

Security Tools
Vuln scanners
Password audit

About
About/Contact
Privacy