Creative Contact Form 4.6.2 Directory Traversal

Authored by Wolfgang Hotwagner

Posted Mar 8, 2020

Creative Contact Form version 4.6.2 before Dec 03 2019 suffers from a directory traversal vulnerability.

tags | exploit
advisories | CVE-2020-9364
SHA-256 | aeb7f30880b5478f81755ab88a32b1174ba8a88701892c3ea6ca776d774d36f6 Download | Favorite | View

Related Files

Share This

Like Twee LinkedIn Reddit Digg StumbleUpon

Change Mirror Download

```
# Directory Traversal in Creative Contact Form

## Overview
* Identifier: AIT-SA-20200301-01
* Target: Creative Contact Form (for Joomla)
* Vendor: Creative Solutions
* Version: 4.6.2 (before Dec 03 2019)
* CVE: CVE-2020-9364
* Accessibility: Remote
* Severity: Critical
* Author: Wolfgang Hotwagner (AIT Austrian Institute of Technology)

## Summary
[Creative Contact Form](https://creative-solutions.net/) is a responsive jQuery contact form for the Joomla
content-management-system.

## Vulnerability Description
A directory traversal vulnerability resides inside the mailer component of the Creative Contact Form for
Joomla. An attacker could exploit this vulnerability to receive any files from the server via e-mail.

The vulnerable code is located in "helpers/mailer.php" at line 290:
```
if(isset($_POST['creativecontactform_upload'])) {
if(is_array($_POST['creativecontactform_upload'])) {
foreach($_POST['creativecontactform_upload'] as $file) {

// echo $file.'--';
$file_path = JPATH_BASE . '/components/com_creativecontactform/views/creativeupload/files/'.$file;
$attach_files[] = $file_path;
}
}
}
```

If an attacker puts "../../../../../../../../etc/passwd" into $_POST['creativecontactform_upload'], and enables
"Send me a copy", the contact-form would send him the content of /etc/passwd via email.

_Note: this vulnerability might not be exploitable in the free version of Creative Contact Form since it does
not allow "Send copy to sender"._

## Vulnerable Versions
Creative Contact Form Personal/Professional/Business 4.6.2 (before Dec 3 2019)

## Impact
An unauthenticated attacker could receive any file from the server

## Mitigation
Update to the current version

## References:
*  https://nvd.nist.gov/vuln/detail/CVE-2020-9364

## Vendor Contact Timeline

* `2019-12-02` Contacting the vendor
* `2019-12-02` Vendor published a fixed version
* `2019-03-01` Public disclosure

## Advisory URL
[https://www.ait.ac.at/ait-sa-20200301-01-directory-traversal-in-creative-contact-form]
(https://www.ait.ac.at/ait-sa-20200301-01-directory-traversal-in-creative-contact-form)
```


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