[AIT-SA-20200301-01] CVE-2020-9364: Directory Traversal in Creative Contact Form

From: sec-advisory <sec-advisory () ait ac at>
Date: Wed, 4 Mar 2020 12:40:57 +0000

```
# 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)


_____
Sent through the Full Disclosure mailing list
https://nmap.org/mailman/listinfo/fulldisclosure
Web Archives & RSS: http://seclists.org/fulldisclosure/
```

By Date By Thread

Current thread:

[AIT-SA-20200301-01] CVE-2020-9364: Directory Traversal in Creative Contact Form ***sec-advisory (Mar 06)***

Site Search

Nmap Security Scanner
Ref Guide
Install Guide
Docs
Download
Nmap OEM

Npcap packet capture
User's Guide
API docs
Download
Npcap OEM

Security Lists
Nmap Announce
Nmap Dev
Full Disclosure
Open Source Security
BreachExchange

Security Tools
Vuln scanners
Password audit
Web scanners
Wireless
Exploitation

About
About/Contact
Privacy
Advertising
Nmap Public Source License