Accessibility: Remote
Severity: High
Author: Wolfgang Hotwagner (AIT Austrian Institute of Technology)

SUMMARY

Creative Contact Form 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

SOLUTION

Update to the current version

REFERENCES

- https://nvd.nist.gov/vuln/detail/CVE-2020-9364 (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
2020-03-01	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)

WOLFGANG HOTWAGNER

Research Engineer /
Security & Communication Technologies

☎ +43 664 88335483 (tel:+43 664 8833 5483)

+43 50550-4150

✉ wolfgang.hotwagner(at)ait.ac.at (mailto:wolfgang.hotwagner@ait.ac.at)

(/)

AIT AUSTRIAN INSTITUTE OF TECHNOLOGY GMBH

Giefinggasse 4
1210 Vienna
Austria

office@ait.ac.at (mailto:office@ait.ac.at)
+43 50550-0 (tel:+4350550-0)

Impressum (/impressum)

NAVIGATION

Über das AIT (/ueber-das-ait)
Themen (/themen)
Lösungen (/loesungen)
Publikationen (/publikationen)
Media (/media)
News & Events (/news-events)
Karriere (/karriere)
Kontakt (/kontakt)

FOLLOW US

YouTube (https://www.youtube.com/user/AITTomorrowToday)
Twitter (https://twitter.com/aittomorrow2day)
Facebook (https://www.facebook.com/AITtomorrow2day/)
LinkedIn (https://www.linkedin.com/company/austrian-institute-of-technology/)
ResearchGate (https://www.researchgate.net/institution/AIT-Austrian-Institute-of-Technology)
AIT Newsletter (/news-events/ait-newsletter)
AIT-Blog (https://www.ait.ac.at/blog)
AIT-Podcast (https://open.spotify.com/show/4ZAdiTs8KcJXH3c8NfQeES)
AIT-Podcast (https://soundcloud.com/user-378778548)

LINKS

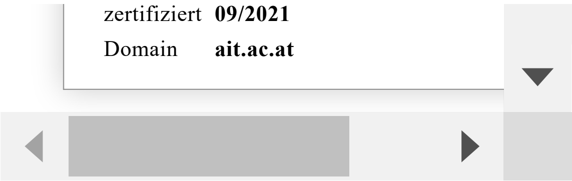
Sitemap (/sitemap)
Standorte und Tochterunternehmen (/ueber-das-ait/standorte-und-tochterunternehmen)
AGB (/agb)
Zertifizierungen (/ueber-das-ait/zertifizierungen)
Akkreditierung (/ueber-das-ait/akkreditierung)
Disclaimer & Data Protection (/disclaimer-data-protection)
Barrierefreiheit (/barrierefreiheit)
Incident Reporting (/incident-reporting)
Covid-19 Schutzmaßnahmen (/fileadmin/user_upload/Infoblatt_COVID-19_Besuchende_Extern.pdf)

WACA Web Accessibility Certificate Austria
www.waca.at

Anrufen (tel:0043505500)

E-Mail

Standorte (/ueber-das-ait/standorte-und-tochterunternehmen)



zertifiziert **09/2021**
Domain **ait.ac.at**