1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\tmpl\commontemplates\errorhandler.php*(8.21K)(Date dernière modif. September 21 2024 09:12:44.)*2ce85090fd569a36e4bdc4feed9d8526**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **5722** du fichier; voici le contexte :
2. T, true)) ?></pre>
3. <h4>$\_POST</h4>
4. <pre><?= htmlentities(print\_r($\_POST, true)) ?></pre>
5. <h4>$**\_COOKIE**</h4>
6. <pre><?= htmlentities(print\_r($**\_COOKIE**, true)) ?></pre>
7. <h4>$\_REQUEST</h4>

<pre><?= html

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_COOKIE**Trouvé en position **5768** du fichier; voici le contexte :

= htmlentities(print\_r($\_POST, true)) ?></pre>

<h4>$**\_COOKIE**</h4>

<pre><?= htmlentities(print\_r($**\_COOKIE**, true)) ?></pre>

<h4>$\_REQUEST</h4>

<pre><?= htmlentities(print\_r($\_REQUEST, true)) ?></pre>

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\tmpl\controlpanel\warnings.php*(11.37K)(Date dernière modif. September 21 2024 09:12:44.)*c902cf5dff7ecf12251b3a2d352a6b22**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **XSECURITY**Trouvé en position **4269** du fichier; voici le contexte :
2. success w-100">
3. <span class="fa fa-hammer"></span>
4. <?= Text::\_('COM\_AKEEBABACKUP\_CPANEL\_BTN\_FI**XSECURITY**') ?>
5. </button>
6. </form>
7. <?php else: ?>
8. <p>

<?= Text::\_('COM\_AKEEBABACKUP\_CPANEL\_LBL\_OUTDIR\_TR

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **XSECURITY**Trouvé en position **5410** du fichier; voici le contexte :

success w-100">

<span class="fa fa-hammer"></span>

<?= Text::\_('COM\_AKEEBABACKUP\_CPANEL\_BTN\_FI**XSECURITY**') ?>

</button>

</form>

</details>

<?php // mbstring warning ?>

<?php if(!$this->checkMbstring)

1. D: \wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Core\Domain\Finalizer\PostProcessing.php*(9.71K)(Date dernière modif. September 21 2024 09:12:44.)*2a19f3c5171bbc87e7447714af3af9b2**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **remote file upload**Trouvé en position **1302** du fichier; voici le contexte :
2. use Exception;
3. use Akeeba\Engine\Psr\Log\LogLevel;
4. /\*\*
5. \* Performs any necessary post-processing (**remote file upload**ing) still pending.
6. \*
7. \* @since 9.3.1
8. \* @package Akeeba\Engine\Core\Domain\Finalizer

\*

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Complexify.php*(15.49K)(Date dernière modif. September 21 2024 09:12:44.)*cde1af865d468519c69b8bf3c3144037**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **warrior**Trouvé en position **9780** du fichier; voici le contexte :
2. hannon', 'success', 'testing', 'thunder',
3. 'thx1138', 'tiffany', 'trouble', 'twitter', 'voyager', '**warrior**', 'welcome',
4. 'william', 'winston', 'yankees', 'zxcvbnm', '11111111', '12345678', 'access14',

'b

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_akeebabackup\vendor\akeeba\engine\engine\Util\Statistics.php*(7.33K)(Date dernière modif. September 21 2024 09:12:44.)*22823499e280d025849a9c27a4982c08**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **brute force**Trouvé en position **3918** du fichier; voici le contexte :
2. filename))
3. {
4. $ret[] = $filename;
5. }
6. }
7. // Edge case: still running backups, we have to **brute force** the scan
8. // of existing files (multipart may be lying)
9. if ($stat['status'] == 'run')
10. {

$ba

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_icagenda\CHANGELOG.php*(398.89K)(Date dernière modif. August 28 2024 17:48:10.)*9b44567eaab6d5f826257341ceadcf38**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **SQL injection**Trouvé en position **163961** du fichier; voici le contexte :
2. .0 through 3.7.13
3. 1 Description: The lack of type casting of a variable in SQL statement leads to a **SQL injection** vulnerability in the events list view.

+ Added : Search in custom fields value with the frontend gl

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_jce\vendor\Defuse\Crypto\Crypto.php*(13.99K)(Date dernière modif. August 31 2024 15:58:02.)*77bfdbf16d0f59a615ec9c702c6e9eaf**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **1070** du fichier; voici le contexte :
2. \* Encrypts a string with a password, using a slow key derivation function
3. \* to make password **cracking** more expensive.
4. \*
5. \* @param string $plaintext
6. \* @param string $password

\* @param

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **3258** du fichier; voici le contexte :

iphertext to a string with a password, using a slow key

\* derivation function to make password **cracking** more expensive.

\*

\* @param string $ciphertext

\* @param string $password

\* @para

×

1. D:\wamp64\www\randophil56.j5.local\administrator\components\com\_jce\vendor\Defuse\Crypto\File.php*(24.92K)(Date dernière modif. August 31 2024 15:58:02.)*1a0b019a98d21149a6c4c691e5c58969**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **742** du fichier; voici le contexte :
2. \* Encrypts a file with a password, using a slow key derivation function to
3. \* make password **cracking** more expensive.
4. \*
5. \* @param string $inputFilename

\* @param string $outputFilename

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **1967** du fichier; voici le contexte :

\* Decrypts a file with a password, using a slow key derivation function to

\* make password **cracking** more expensive.

\*

\* @param string $inputFilename

\* @param string $outputFilename

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **3310** du fichier; voici le contexte :

e handle into another with a

\* password, using a slow key derivation function to make password **cracking**

\* more expensive.

\*

\* @param resource $inputHandle

\* @param resource $outputHan

**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **cracking**Trouvé en position **4684** du fichier; voici le contexte :

resource into another with a password, using

\* a slow key derivation function to make password **cracking** more expensive.

\*

\* @param resource $inputHandle

\* @param resource $outputHandle

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\libraries\classes\editor.php*(45.22K)(Date dernière modif. August 31 2024 15:58:02.)*4d9552ff967310e74f9f11586fba09fe**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **12344** du fichier; voici le contexte :
2. lode(',', $stylesheets);
3. // use cookies to store state
4. $settings['use\_state**\_cookie**s'] = (bool) $wf->getParam('editor.use**\_cookie**s', 1);
5. // Set active tab

$set

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **12389** du fichier; voici le contexte :

cookies to store state

$settings['use\_state**\_cookie**s'] = (bool) $wf->getParam('editor.use**\_cookie**s', 1);

// Set active tab

$settings['active\_tab'] = 'wf-editor-' . $wf->get

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\libraries\classes\manager\base.php*(8.81K)(Date dernière modif. August 31 2024 15:58:02.)*937df2eeda429d16c920b6600fd052e4**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **8718** du fichier; voici le contexte :
2. filebrowser\_position', $this->getParam('editor.browser\_position', 'bottom')),
3. 'use\_state**\_cookie**s' => $this->getParam('editor.use**\_cookie**s', true),

'search\_depth' => $this->getParam('ed

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **8758** du fichier; voici le contexte :

editor.browser\_position', 'bottom')),

'use\_state**\_cookie**s' => $this->getParam('editor.use**\_cookie**s', true),

'search\_depth' => $this->getParam('editor.filebrowser\_search\_depth', 3),

×

1. D:\wamp64\www\randophil56.j5.local\components\com\_jce\editor\libraries\classes\mobile.php*(86.72K)(Date dernière modif. October 04 2023 16:06:24.)*6260e844bd234c942dd99b1d07c6c8ba**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **ia\_archiver**Trouvé en position **56614** du fichier; voici le contexte :

L|s~amp-validator|AdsBot-Google|Google Keyword Suggestion|Facebot|YandexBot|YandexMobileBot|bingbot|**ia\_archiver**|AhrefsBot|Ezooms|GSLFbot|WBSearchBot|Twitterbot|TweetmemeBot|Twikle|PaperLiBot|Wotbox|UnwindFetchor

1. D:\wamp64\www\randophil56.j5.local\modules\mod\_jm\_kick\_cass\tmpl\default.php*(23.73K)(Date dernière modif. March 26 2022 14:53:54.)*b390f510efd2f44038bf0c5380a6afab**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **510** du fichier; voici le contexte :
2. tInstance();
3. $base=$uri->base();
4. $cc\_textdecoration = $params->get('textdedoration', '0');
5. $cc**\_cookie**notice = $params->get('CookieNotice');
6. $cc\_popup = $params->get('Popup');

$cc\_s

**Danger** Ce mot est un mot ayant été encodé en base64 et correspondant à une mot réservé de php comme p.ex. $\_SERVER ou $\_COOKIES. Il y a de fortes chances qu'il s'agisse d'un code malsain.Signature : **\_cookie**Trouvé en position **6726** du fichier; voici le contexte :

ho $params->get('ShareNumber')?>

}

});

};

</script>

<?php

}

if ($cc**\_cookie**notice){

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*//

//\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

1. D:\wamp64\www\randophil56.j5.local\plugins\system\jsvisit\_counter\helper.php*(41.72K)(Date dernière modif. July 15 2024 18:05:06.)*91f496ab02587be313cac66f24236e65**Danger** Forte probabilité qu'il s'agisse d'un fichier ayant été virusé ou étant un virusSignature : **ia\_archiver**Trouvé en position **16372** du fichier; voici le contexte :
2. $bots = array(
3. 'Googlebot',
4. 'Baiduspider',
5. '**ia\_archiver**',
6. 'R6\_FeedFetcher',
7. 'NetcraftSurveyAgent',

'Sogo