**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 29 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Helpers.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$manifest = json\_decode(file\_get\_contents($manifestFile), true);

**STANDARD: Potentially Unsafe Code - passthru**

Line: 298 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Console\Commands\InitCommand.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

passthru($command, $status);

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 298 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Console\Commands\InitCommand.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

passthru($command, $status);

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Http\Controllers\API\SettingController.php

@TODO: This should be a PUT request

**STANDARD: Potentially Unsafe Code - preg\_replace**

Line: 36 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Repositories\AbstractRepository.php

This function will evaluate PHP code. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

return preg\_replace('/(.+)\\\\Repositories\\\\(.+)Repository$/m', '$1\Models\\\$2', static::class);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 236 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\FileSynchronizer.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->mediaMetadataService->writeAlbumCover($album, file\_get\_contents($cover), $extension);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 250 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\FileSynchronizer.php

MD5 Hashing algorithm.

return $this->cache->remember(md5($this->filePath . '\_cover'), 24 \* 60, function (): ?string {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 13 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\HelperService.php

MD5 Hashing algorithm.

return md5(config('app.key') . $path);

**MEDIUM: Potentially Unsafe Code - md5**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\ITunesService.php

MD5 Hashing algorithm.

md5("itunes\_track\_url\_{$term}{$album}{$artist}"),

**MEDIUM: Potentially Unsafe Code - md5**

Line: 44 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\LastfmService.php

MD5 Hashing algorithm.

return $this->cache->remember(md5("lastfm\_artist\_$name"), 24 \* 60 \* 7, function () use ($name): ?array {

**MEDIUM: Potentially Unsafe Code - md5**

Line: 94 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\LastfmService.php

MD5 Hashing algorithm.

$cacheKey = md5("lastfm\_album\_{$albumName}\_{$artistName}");

**MEDIUM: Potentially Unsafe Code - md5**

Line: 260 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\LastfmService.php

MD5 Hashing algorithm.

$params['api\_sig'] = md5($str);

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 27 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\MediaMetadataService.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->writeAlbumCover($album, file\_get\_contents($imageUrl), last($extension));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 64 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\MediaMetadataService.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

$this->writeArtistImage($artist, file\_get\_contents($imageUrl), last($extension));

**LOW: Potentially Unsafe Code - Variable Used as FileName**

Line: 135 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\MediaMetadataService.php

The application appears to use a variable name in order to define a filename used by the application. It is unclear whether this variable can be controlled by the user - carry out a manual inspection to confirm.

file\_get\_contents($album->cover\_path),

**MEDIUM: Potentially Unsafe Code - md5**

Line: 58 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\YouTubeService.php

MD5 Hashing algorithm.

return $this->cache->remember(md5("youtube\_$uri"), 60 \* 24 \* 7, function () use ($uri) {

**MEDIUM: Potentially Unsafe Code - Potential XSS**

Line: 35 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\Streamers\PhpStreamer.php

The application appears to reflect data to the screen with no apparent validation or sanitisation. It was not clear if this variable is controlled by the user.

echo "An error occurred while attempting to send the requested resource: {$e->getMessage()}";

**SUSPICIOUS COMMENT: Comment Indicates Potentially Unfinished Code -**

Line: 28 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\Streamers\Streamer.php

or even Symfony's MIMETypeGuesser, since they appear to be wrong sometimes.

**STANDARD: Potentially Unsafe Code - passthru**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\Streamers\TranscodingStreamer.php

This function allows execution of commands. It is dangerous when used with user controlled parameters and may facilitate direct attacks against the web server. Conduct a manual review of this section to ensure safe usage.

passthru("$ffmpeg " . implode(' ', $args));

**MEDIUM: Potentially Unsafe Code - Application Variable Used on System Command Line**

Line: 47 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\app\Services\Streamers\TranscodingStreamer.php

The application appears to allow the use of an unvalidated variable when executing a command. Carry out a manual check to determine whether the variable is user-controlled.

passthru("$ffmpeg " . implode(' ', $args));

**MEDIUM: Potentially Unsafe Code - md5**

Line: 19 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\database\factories\AlbumFactory.php

MD5 Hashing algorithm.

'cover' => md5(uniqid()) . '.jpg',

**MEDIUM: Potentially Unsafe Code - md5**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\database\factories\ArtistFactory.php

MD5 Hashing algorithm.

'image' => md5(uniqid()) . '.jpg',

**STANDARD: Potentially Unsafe Code - system**

Line: 17 - C:\Users\Jeremy\OneDrive\Desktop\Downloads\CVE 2021 33563\Buggy\koel-5.1.4\koel-5.1.4\resources\views\errors\template.blade.php

This function allows execution of commands. It is dangerous with user controlled parameters and may facilitate direct attacks against the web server.

font-family: system, -apple-system, BlinkMacSystemFont, "Segoe UI", Roboto, Oxygen-Sans, Ubuntu, Cantarell, "Helvetica Neue", sans-serif;