WorePress의 ProfilePress 플러그인에서 발생하며 사용자 등록을 할 때 사용자가 권한 상승을 하여 관리자로 등록할 수 있는 취약점

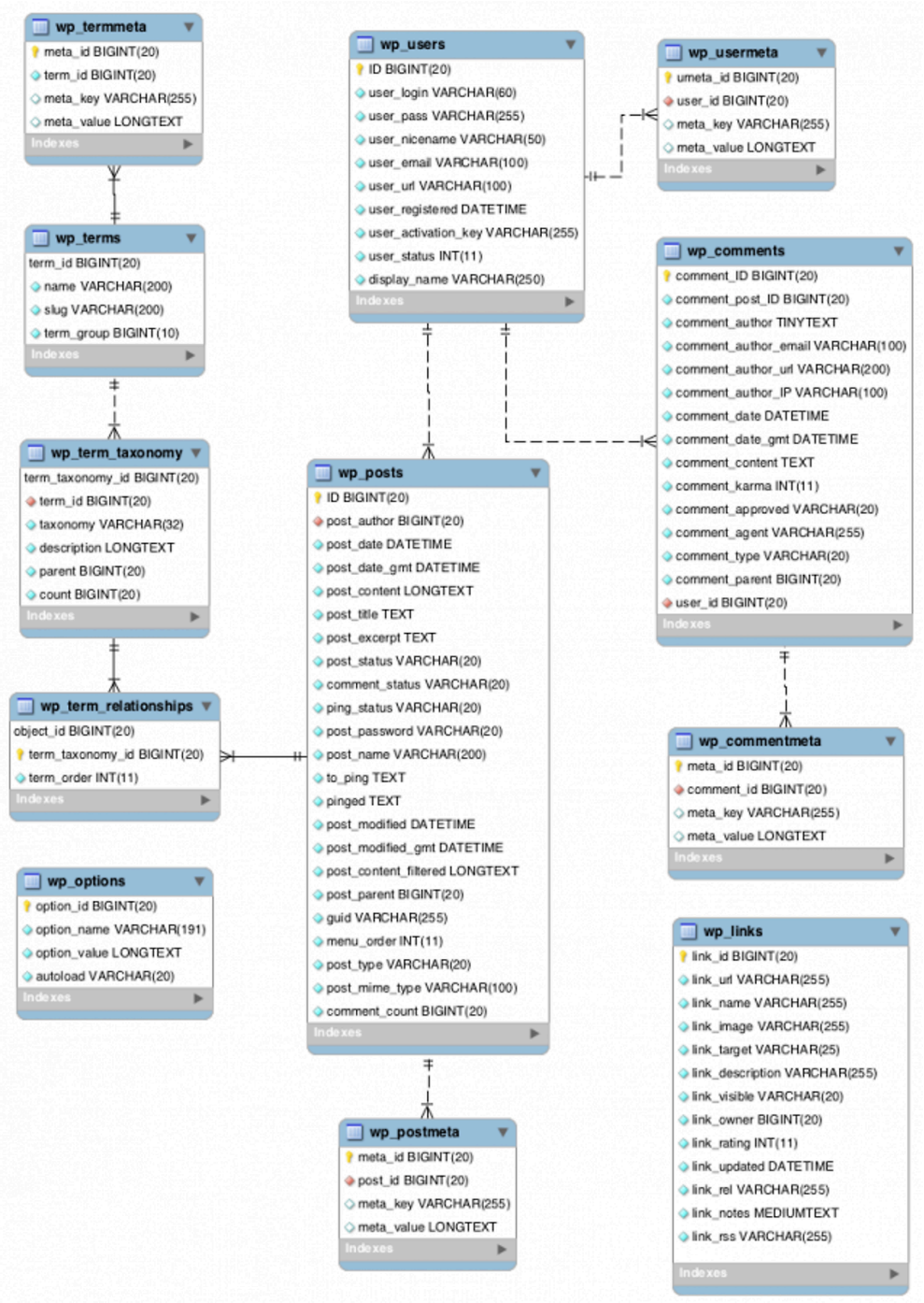
취약한 버전

ProfilePress 3.0 - 3.1.3

ProfilePress Plugin ?

취약점 발견 당시 활성 설치수가 400,000이 넘는 플러그인으로 전자상거래, 사용자 등록 양식, 로그인 양식, 멤버십 기능을 제공

WordPress DataBase



- wp_termmeta, wp_terms, wp_users, wp_usermeta, wu_posts 등 다양한 테이블로 나누어져 있음

WP_USERS

- 사이트에 등록된 모든 사용자를 저장하는 기본 테이블
- 암호화 된 비밀번호, 이메일, 등록 시간 등

WP_USERMETA

- 임의의 정보를 저장하기 위한 추가 테이블
- 사용자의 추가 데이터를 저장하고 wp_users 테이블을 확장
- 사용자 이름, 사용자의 권한 등

WP_CAPABILITY

wp_usermeta 테이블에 저장되는 메타 데이터 값 중 하나로 사용자의 권한을 설정

데이터 예시>
데이터는 직렬화되어 저장

```
user1
a:8:{s:13:"administrator";b:1;
s:14:"frm_view_forms";b:1;
s:14:"frm_edit_forms";b:1;
s:16:"frm_delete_forms";b:1;
s:19:"frm_change_settings";b:1;
s:16:"frm_view_entries";b:1;
s:18:"frm_delete_entries";b:1;
s:16:"tutor_instructor";b:1;}
```

역직렬화를 통해 데이터 확인

```
array(
'administrator' => true,
'frm_view_forms' => true,
'frm_edit_forms' => true,
'frm_delete_forms' => true,
'frm_change_settings' => true,
'frm_view_entries' => true,
'frm_delete_entries' => true,
'tutor_instructor' => true
);
```

동작 과정

1. 취약한 버전인 ProfilePress 3.0 - 3.1.3 버전 플러그인을 설치한다.
2. 가입 페이지를 활성화 하기 위해 Settings > General의 Membership에서 Anyone can register를 체크한다.
3. 활성화 된 Sign Up 페이지에 들어가 정보를 입력한 후 가입 요청을 보낸다.
4. Burp Suite를 이용해 요청을 가로챈 후 **wp_capabilities[administrator]=1**을 추가 작성한다.
5. 가입 시 권한이 관리자로 부여되어 있는 것을 확인 할 수 있다.

> ⓘ wp_capabilities[administrator]=
>
> wp_capabilities의 값을 1로 설정해주지 않더라도 직렬화된 배열의 구조와 데이터값의 유효성만 검증하기 때문에 키가 존재하기만 하면 권리자 권한을 가졌다고 간주하여 권한 상승이 가능

Patch

ProfilePress 3.1.4 버전에서 수정
취약 코드 /src/Classes/RegistrationAuth.php에 if문을 추가하여 입력 값이 적절한지 검증
ppress_custom_fileds_key_value_pair() 함수를 통해 검증하고 true일 경우에만 $custom_usermeta에 저장

-avatar/tags/3.1.4/src/Classes/RegistrationAuth.php Tabular

3035724

```
92      * @param string $no_login_redirect
93      *
        * @return string
94      * @return string|void
95      */
96     public static function register_new_user($post, $form_id = 0, $redirect = '', $is_melange = false, $no_login_redirect = '')
97     {
98         if ( ! get_option('users_can_register')) return;
99
100        $files = $_FILES;
101
...
239        // get the data for use by update_meta
240        $custom_usermeta = array();
           // loop over the $_POST data and create an array of the invalid userdata/ custom usermeta
           foreach ($post as $key => $value) {
               if ($key == 'reg_submit' || in_array($key, ppress_reserved_field_keys())) continue;

               if ( ! in_array($key, $valid_userdata)) {
                   $custom_usermeta[$key] = is_array($value) ? array_map('sanitize_text_field', $value) : sanitize_text_field($value);
241
242        if (ExtensionManager::is_premium()) {
243            // loop over the $_POST data and create an array of the invalid userdata/ custom usermeta
244            foreach ($post as $key => $value) {
245
246                if ($key == 'reg_submit' || in_array($key, ppress_reserved_field_keys())) continue;
247
248                if ( ! in_array($key, $valid_userdata)) {
249
250                    if (in_array($key, array_keys(ppress_custom_fields_key_value_pair(true)))) {
251                        $custom_usermeta[$key] = is_array($value) ? array_map('sanitize_text_field', $value) : sanitize_text_field($value);
252                    }
253                }
```

---

https://myungjjju.tistory.com/319

https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-34621