Chloe Chamberland

November 9, 2020

Critical Privilege Escalation Vulnerabilities Affect 100K Sites Using Ultimate Member Plugin

On October 23, 2020, our Threat Intelligence team responsibly disclosed several vulnerabilities in Ultimate Member, a WordPress plugin installed on over 100,000 sites. These flaws made it possible for attackers to escalate their privileges to those of an administrator and take over a WordPress site.

We initially reached out to the plugin's developer on October 23, 2020. After establishing an appropriate communication channel, we provided the full disclosure details on October 26, 2020. The developer provided us with a copy of the first intended patch on October 26, 2020 for us to test. We confirmed the patch fixed one of the vulnerabilities, however, two still remained. On October 29, 2020, the plugin's developer provided us with an updated copy which fully addressed all vulnerabilities. The plugin's developer released a patched version of Ultimate Member, 2.1.12, on October 29, 2020.

These are critical and severe vulnerabilities that are easy to exploit. Therefore, **we highly recommend updating to the patched version, 2.1.12, immediately.**

Wordfence Premium users received a firewall rule to protect against any exploits targeting these vulnerabilities on October 23, 2020. Sites still using the free version of Wordfence will receive the same protection on November 22, 2020.

Unauthenticated Privilege Escalation via User Meta

Description: Privilege Escalation
Affected Plugin: Ultimate Member
Plugin Slug: ultimate-member
Affected Versions: <= 2.1.11
CVE ID: CVE-2020-36155
CVSS Score: 10.0 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Fully Patched Version: 2.1.12

Ultimate Member is a popular plugin designed to enhance user registration and account control on WordPress sites. It allows site owners to create custom roles and manage the privileges of site members. As part of its functionality, the plugin automatically creates three forms: user registration, user login, and user profile management.

We discovered that the user registration form lacked some checks on submitted user data. This oversight made it possible for an attacker to supply arbitrary user meta keys during the registration process that would update those meta keys in the database. This meant that an attacker could supply an array parameter for sensitive meta data such as the `wp_capabilities` user meta which defines a user's role. During the registration process, submitted registration details were passed to the `update_profile` function, and any respective metadata that was submitted, regardless of what was submitted, would be updated for that newly registered user.

```
1195 do_action( 'um_before_save_registration_details', $this->id, $submitted );
1196
1197             update_user_meta( $this->id, 'submitted', $submitted );
1198
1199             $this->update_profile( $submitted );
```

```
1809 function update_profile( $changes ) {
1810
1811             $args['ID'] = $this->id;
```

```
1835 $changes = apply_filters( 'um_before_update_profile', $changes, $args['ID'] );
1836
1837             foreach ( $changes as $key => $value ) {
1838                 if ( ! in_array( $key, $this->update_user_keys ) ) {
1839                     if ( $value === 0 ) {
1840                         update_user_meta( $this->id, $key, '0' );
1841                     } else {
1842                         update_user_meta( $this->id, $key, $value );
1843                     }
1844                 } else {
1845                     $args[ $key ] = esc_attr( $changes[ $key ] );
1846                 }
1847             }
```

This meant that an attacker simply needed to supply `wp_capabilities[administrator]` as part of a registration request, and that attacker would effectively update the `wp_capabilities` field with the administrator role. This simple request would grant administrator access upon registration.

This vulnerability is considered very critical as it makes it possible for originally unauthenticated users to easily escalate their privileges to those of an administrator. Once an attacker has administrative access to a WordPress site, they have effectively taken over the entire site and can perform any action, from taking the site offline to further infecting the site with malware.

Unauthenticated Privilege Escalation via User Roles

Affected Plugin: Ultimate Member
Plugin Slug: ultimate-member
Affected Versions: <= 2.1.11
CVE ID: CVE-2020-36157
CVSS Score: 10.0 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H
Fully Patched Version: 2.1.12

This vulnerability is related to the previously detailed vulnerability. Due to the lack of filtering on the role parameter that could be supplied during the registration process, an attacker could supply the role parameter with a WordPress capability or any custom Ultimate Member role and effectively be granted those privileges. After updating the user meta, the plugin checked if the role parameter was supplied. If so, a few checks were processed to verify the role being supplied.

```
// update user
            if ( count( $args ) > 1 ) {
                //if isset roles argument validate role to properly for security reasons
                if ( isset( $args['role'] ) ) {
                    global $wp_roles;
                    $um_roles = get_option( 'um_roles' );

                    if ( ! empty( $um_roles ) ) {
                        $role_keys = array_map( function( $item ) {
                            return 'um_' . $item;
                        }, get_option( 'um_roles' ) );
                    } else {
                        $role_keys = array();
                    }

                    $exclude_roles = array_diff( array_keys( $wp_roles->roles ), array_merge( $role_keys, array( 'su

                    if ( in_array( $args['role'], $exclude_roles ) ) {
                        unset( $args['role'] );
                    }
                }

                wp_update_user( $args );
            }

        }
```

Fortunately, the plugin blocked default WordPress roles from being supplied in the role parameter making it more difficult for attackers to be able to exploit this vulnerability to gain escalated privileges. In addition, if the role selector was enabled for the registration form, then only the roles specified by the site administrator could be selected and supplied during registration.

However, it did not stop custom Ultimate Member roles from being supplied or individual WordPress capabilities prior to updating the user role. Therefore, despite the initial protections, an attacker could still easily gain elevated privileges.

Attackers could enumerate the current custom Ultimate Members roles and supply a higher privileged role while registering in the role parameter. Or, an attacker could supply a specific capability and then use that to switch to another user account with elevated privileges. In either case, if wp-admin access was enabled for that user or role, then this vulnerability could be used in conjunction with the final vulnerability detailed below.

Again, this vulnerability is considered critical as it allows originally unauthenticated users to escalate their privileges with some conditions. Once an attacker has elevated access to a WordPress site, they can potentially take over the entire and further infect the site with malware.

Authenticated Privilege Escalation via Profile Update

Description: Privilege Escalation
Affected Plugin: Ultimate Member
Plugin Slug: ultimate-member
Affected Versions: <= 2.1.11
CVE ID: CVE-2020-36156
CVSS Score: 9.9 (CRITICAL)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H
Fully Patched Version: 2.1.12

This final vulnerability was introduced due to a lack of capability checks on a profile update. Due to the fact that Ultimate Member allowed the creation of new roles, this plugin also made it possible for site administrators to grant secondary Ultimate Member roles for all users. This was intended to allow a user to have default privileges for a built-in role, such as editor, but also have additional secondary privileges to extend capabilities of a membership site using Ultimate Member. The plugin uses a function, `profile_update` which runs whenever a user's profile is updated to update the Ultimate Member role for any given user. This function used `is_admin()` alone without a capability check, making it possible for any user to supply the um-role post field and set their role to one of their choosing.

```
            function profile_update( $user_id, $old_data ) {
            // Bail if no user ID was passed
            if ( empty( $user_id ) ) {
                return;
            }

            $old_roles = $old_data->roles;
            $userdata  = get_userdata( $user_id );
            $new_roles = $userdata->roles;

            if ( is_admin() ) {
                if ( ! empty( $_POST['um-role'] ) ) {
                    $new_roles = array_merge( $new_roles, array( $_POST['um-role'] ) );
                    if ( ! user_can( $user_id, $_POST['um-role'] ) ) {
                        UM()->roles()->set_role( $user_id, $_POST['um-role'] );
                    }
                }
            }
}
            }
```

This meant that any user with wp-admin access to the profile.php page, whether explicitly allowed or via another vulnerability used to gain that access, could supply the parameter `um-role` with a value set to any role including `administrator` during a profile update and effectively escalate their privileges to those of that role.

As with the previous vulnerabilities outlined above, this vulnerability is considered critical as it makes it possible for authenticated users to escalate their privileges with very little difficulty. Once an attacker has administrator privileges on a WordPress site, they have effectively taken over the entire site.

Disclosure Timeline

- **October 19-23, 2020 –** Initial discovery of one vulnerability and further investigation of the plugin which leads to discovery of two more vulnerabilities.
- **October 23, 2020** – We develop a firewall rule to protect Wordfence customers and release it to Wordfence Premium users. We initiate contact with the plugin's developer.
- **October 26, 2020** – The plugin's developer confirms the inbox for handling discussion. We send full disclosure.
- **October 26, 2020** – The plugin's developer confirms the vulnerability and provides us with a patched copy to verify the fixes. We inform them that some flaws still exist.
- **October 29, 2020** – The plugin's developer provides us with a second patched copy to verify the additional fixes. We verify that all has been patched.
- **October 29, 2020** – The patch is released in version 2.1.12.
- **November 22, 2020** – Free Wordfence users receive firewall rule.

Conclusion

ability to escalate their privileges in various different ways. These flaws have been fully patched in version 2.1.12. We recommend that users immediately update to the latest version available, which is version 2.1.12 at the time of this publication.

Wordfence Premium users received firewall rules protecting against these vulnerabilities on October 23, 2020, while those still using the free version of Wordfence will receive the same protection on November 22, 2020.

If you know a friend or colleague who is using this plugin on their site, we highly recommend forwarding this advisory to them to help keep their sites protected as these are high severity vulnerabilities that are trivial to exploit.

Did you enjoy this post? Share it!

Comments

4 Comments

Christine *
November 10, 2020
4:34 am

I was blocked from using my site two days ago. It showed "code 403". Do I correct this by buying the premium version of word fence?
How do I get the patch for the "Ultimate Member" plugin?
I would appreciate your help as I need to post my tai chi class offerings and am not being allowed to do so.

Kathy Zant *
November 10, 2020
5:41 am

Hi Christine, you don't need to buy premium to solve the 403 blocking problem. Please reach out to free support on the forums for assistance. https://wordpress.org/support/plugin/wordfence/

Updating Ultimate Member can be done either via the plugin dashboard or via the update dashboard.

Stephen *
November 10, 2020
4:42 am

Thank you very much for your prompt action against attacks. Unfortunately, my site legitebusiness(dot)com has been attacked.

So is the next action to take?

Kathy Zant *
November 10, 2020
5:43 am

If your site is under attack, Wordfence will block those attacks. If you've been compromised and your scan is showing malware, you can clean your site using Wordfence. This guide here should help. https://www.wordfence.com/docs/how-to-clean-a-hacked-wordpress-site-using-wordfence/