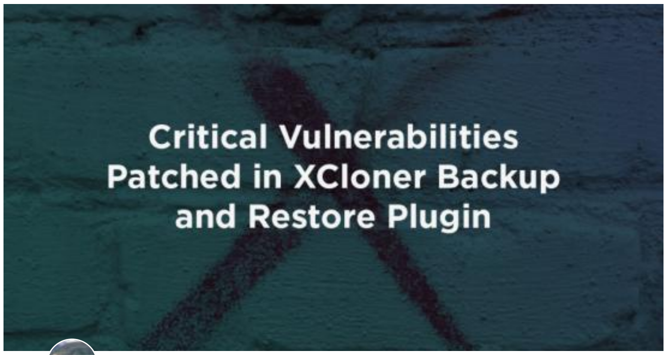

Chloe Chamberland

September 22, 2020

Critical Vulnerabilities Patched in XCloner Backup and Restore Plugin

On August 14, our Threat Intelligence team discovered several vulnerabilities present in XCloner Backup and Restore, a WordPress plugin installed on over 30,000 sites. This flaw gave authenticated attackers, with subscriber-level or above capabilities, the ability to modify arbitrary files, including PHP files. Doing so would allow an attacker to achieve remote code execution on a vulnerable site's server. Alternatively, an attacker could create an exploit chain to obtain a database dump due to the same unprotected AJAX endpoint, amongst other things. The plugin also contained several endpoints that were vulnerable to cross-site request forgery (CSRF).

We initially reached out to the plugin's team on August 17, 2020. After establishing an appropriate communication channel, we provided the full disclosure details on August 18, 2020. The plugin's team quickly released an initial patch on August 19, 2020 to resolve the most severe problem, and they released an additional patch on September 8, 2020 to resolve the remaining issues.

This is considered a critical security issue that could lead to remote code execution on a vulnerable site's server. **If you haven't already updated, we highly recommend updating to the fully patched version, 4.2.153, immediately.**

Wordfence Premium users received a firewall rule on August 17, 2020 to protect against any exploits targeting these vulnerabilities. Sites still using the free version of Wordfence received the same protection on September 17, 2020.

Description: Unprotected AJAX Action to Arbitrary File Overwrite and Sensitive Information Disclosure
Affected Product: XCloner Backup and Restore
Plugin slug: xcloner-backup-and-restore
Affected Versions: 4.2.1 – 4.2.12
CVE ID: CVE-2020-35948
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: 4.2.13

XCloner Backup and Restore is a plugin designed to provide WordPress users with easily customizable backups and simple-to-use restore functionality. Most of the plugin's functionality is powered through the use of various AJAX actions that perform functionality without requiring the page to refresh every time.

```
$this->loader->add_action('wp_ajax_get_database_tables_action', $xcloner_api, 'get_database_tables_action');
$this->loader->add_action('wp_ajax_get_file_system_action', $xcloner_api, 'get_file_system_action');
$this->loader->add_action('wp_ajax_scan_filesystem', $xcloner_api, 'scan_filesystem');
$this->loader->add_action('wp_ajax_backup_database', $xcloner_api, 'backup_database');
$this->loader->add_action('wp_ajax_backup_files', $xcloner_api, 'backup_files');
$this->loader->add_action('wp_ajax_save_schedule', $xcloner_api, 'save_schedule');
$this->loader->add_action('wp_ajax_get_schedule_by_id', $xcloner_api, 'get_schedule_by_id');
$this->loader->add_action('wp_ajax_get_scheduler_list', $xcloner_api, 'get_scheduler_list');
$this->loader->add_action('wp_ajax_delete_schedule_by_id', $xcloner_api, 'delete_schedule_by_id');
$this->loader->add_action('wp_ajax_delete_backup_by_name', $xcloner_api, 'delete_backup_by_name');
$this->loader->add_action('wp_ajax_download_backup_by_name', $xcloner_api, 'download_backup_by_name');
$this->loader->add_action('wp_ajax_remote_storage_save_status', $xcloner_api, 'remote_storage_save_status');
$this->loader->add_action('wp_ajax_upload_backup_to_remote', $xcloner_api, 'upload_backup_to_remote');
$this->loader->add_action('wp_ajax_list_backup_files', $xcloner_api, 'list_backup_files');
$this->loader->add_action('wp_ajax_restore_upload_backup', $xcloner_api, 'restore_upload_backup');
$this->loader->add_action('wp_ajax_download_restore_script', $xcloner_api, 'download_restore_script');
$this->loader->add_action('wp_ajax_copy_backup_remote_to_local', $xcloner_api, 'copy_backup_remote_to_local');
$this->loader->add_action('wp_ajax_restore_backup', $this, 'restore_backup');
$this->loader->add_action('wp_ajax_backup_encryption', $xcloner_api, 'backup_encryption');
$this->loader->add_action('wp_ajax_backup_decryption', $xcloner_api, 'backup_decryption');
$this->loader->add_action('wp_ajax_get_manage_backups_list', $xcloner_api, 'get_manage_backups_list');
```

Nearly all of these AJAX actions were hooked to the `/vendor/watchfulli/xcloner-core/src/Xcloner_Api.php` file which acted as a single functional source file with a corresponding security check used for each function. These functions were protected from unauthorized use by a capability check function `check_access()`.

```
/**
 * Checks API access
 */
public function check_access()
{
    if (function_exists('current_user_can') && !current_user_can('manage_options')) {
        $this->send_response(json_encode("Access not allowed!"));
    }
}
```

However, the AJAX action used to restore back-ups, `wp_ajax_restore_backup`, did not hook to the `Xcloner_Api.php` file, and therefore, did not process the same `check_access()` capability check function even though it was included in the function.

```
$this->loader->add_action('wp_ajax_restore_backup', $this, 'restore_backup');
```

…

```
    /**
     * Restore backup api call
     */
    public function restore_backup()
    {
        $this->check_access();

        define("XCLONER_PLUGIN_ACCESS", 1);
        include_once(dirname(__DIR__).DS."restore".DS."xcloner_restore.php");

        return;
    }
}
```

This meant that low-level users, like subscribers, could trigger this action and use any of the corresponding functions present in the `xcloner_restore.php` file. This consists of the following functions:

- `write_file_action`
- `restore_mysql_backup_action`

- `list_mysqldump_backups_action`
- `list_backup_archives_action`
- `restore_backup_to_path_action`
- `get_current_directory_action`

The most critical function was the `write_file_action` function, which would allow a subscriber-level user the ability to overwrite any files. This functionality could give attackers the ability to overwrite the `wp-config.php` file containing WordPress database credentials and other important settings. Exploiting this vulnerability means an attacker could overwrite the `wp-config.php` to an empty file so that WordPress is tricked into thinking there is a new installation. This would then allow an attacker to connect their own database to an affected site and modify any files once they have re-configured the WordPress installation. Alternatively, an attacker could overwrite any other file with a backdoor and use that to gain access to the website's entire filesystem.

The second most critical function is the `get_current_directory` function, which returns the SQL database credentials for the site, along with the absolute path of the installation. If an attacker could locate public access to the database, then they could log in and steal sensitive information, add an administrative user account, delete posts, or even redirect the site by changing the site url, amongst other malicious activities.

The other plugin actions by themselves have less potential for harm individually, however, an attacker could chain an exploit of these actions together to obtain a SQL database dump. Due to the complexity this type of attack would require, it is unlikely to be actively exploited in the wild.

Description: Cross-Site Request Forgery
Affected Product: XCloner Backup and Restore
Plugin slug: xcloner-backup-and-restore
Affected Versions: <= 4.2.152
CVE ID: Pending.
CVSS Score: 8.8 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H
Fully Patched Version: 4.2.153

In addition to an almost completely unprotected AJAX endpoint, almost all of the endpoints in the plugin were vulnerable to cross-site request forgery due to a failure to implement nonces and corresponding checks.

An attacker could use a CSRF attack to trigger a backup or update plugin options, along with all of the malicious activity outlined above.

Disclosure Timeline

August 14, 2020 – Initial discovery of vulnerable function and further analysis of plugin. Firewall rule creation process begins.
August 17, 2020 – Firewall rule tested and deployed to Wordfence premium users. Initial outreach to the plugin's team.
August 18, 2020 – We send full disclosure details.
August 19, 2020 – An initial patch is released resolving the unprotected AJAX vulnerability.
August 20, 2020 – We follow up to disclose that several endpoints remain with no CSRF protection.
August 28, 2020 – The plugin's team confirms that they are working on the issue and will release a patch shortly.
September 8, 2020 – A final and sufficient patch is released in version 4.2.153.
September 17, 2020 – Wordfence free users receive the firewall rule.

Conclusion

In today's post, we detailed a flaw in the XCloner Backup and Restore plugin that allowed authenticated users to modify arbitrary files and execute any code on the server, as well as several CSRF vulnerabilities. These flaws have been fully patched in version 4.2.153. We recommend that users immediately update to the latest version available, which is version 4.2.153 at the time of this publication.

Sites using Wordfence Premium have been protected from any exploits targeting this vulnerability since August 17, 2020. Sites still running the free version of Wordfence received the same protection on September 17, 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 this is a critical security update.

Did you enjoy this post? Share it!

Comments

No Comments

Our business hours are 9am-8pm ET, 6am-5pm PT and 2pm-1am UTC/GMT excluding weekends and holidays.
Response customers receive 24-hour support, 365 days a year, with a 1-hour response time.

Terms of Service
Privacy Policy
CCPA Privacy Notice

Products
Wordfence Free
Wordfence Premium
Wordfence Care
Wordfence Response
Wordfence Central

Support
Documentation
Learning Center
Free Support
Premium Support

News
Blog
In The News
Vulnerability Advisories

About
About Wordfence
Careers
Contact
Security
CVE Request Form

SIGN UP