‹ Back to all articles

UPDATED: 01.14.2020

Critical Vulnerability In InfiniteWP Client And WP Time Capsule

Dave
from **patchstack**

Not too long ago an authentication bypass vulnerability in the Ultimate Addons was found for Elementor and Beaver Builder plugins.

As we routinely monitor the code of popular plugins our customers use, we found that the InfiniteWP Client and WP Time Capsule plugins also contain logical issues in the code that allows you to login into an administrator account without a password.

The developer was very fast to react and released the patches on the very next day after our initial report. It's always great to see developers who are taking action quickly and letting their customers know about the issues to help people update to a more secure version as soon as possible.

Firewalls may fail to protect

Because authentication bypass vulnerabilities are often logical mistakes in the code and don't actually involve a suspicious-looking payload, it can be hard to find and determine where these issues come from.

In this case, it's hard to block this vulnerability with general firewall rules because the payload is encoded and a malicious payload would not look much different compared to a legitimate-looking payload of both plugins.

We added a new module in the Patchstack firewall just to be able to block this vulnerability as both plugins did not hook into the WordPress core as expected. We have seen other WordPress security companies follow the same method. In the future, we can expand upon this new feature to block similar issues.

Because of the nature of the vulnerability, cloud-based firewalls might not be able to make a difference between malicious or legitimate traffic and therefore may fail to provide effective protection against this vulnerability.

Anyone who uses a firewall by another company should ask them whether or not these particular vulnerabilities are blocked by their firewall.

InfiniteWP Client < 1.9.4.5

In order for the request to even get to the vulnerable part of the code, we first must encode the payload with JSON, then Base64, then send it raw to the site in a POST request.

All we need to know is the username of an administrator on the site. After the request has been sent, you will automatically be logged in as the user.

The issue resides in the function iwp_mmb_set_request which is located in the init.php file. This function checks if the request_params variable of the class IWP_MMB_Core is not empty, which is only populated when the payload meets certain conditions.

In this case, the condition is that the iwp_action parameter of the payload must equal readd_site or add_site as they are the only actions that do not have an authorization check in place. The missing authorization check is the reason why this issue exists.

As you can see, the only change they have made is that the add_site and readd_site actions will no longer populate the request_params variable but return early in the function.

Based on the WordPress plugin library, the InfiniteWP Client plugin is active on 300,000+ websites. The InfiniteWP site claims they have 513,520 sites active.

WP Time Capsule < 1.21.16

The WP Time Capsule plugin does not require a more complex payload but only needs to contain a certain string in the body of the raw POST request.

The issue is located in wptc-cron-functions.php line 12 where it parses the request. The parse_request function calls the function decode_server_request_wptc which check if the raw POST payload contains the string "IWP_JSON_PREFIX".

If it contains this string, it calls wptc_login_as_admin (which grabs all available administrator accounts and uses the first account in the list) and you'll be logged in as an administrator as shown below.

They removed several calls to the wptc_login_as_admin function and made a change so the authenticity of the payload is verified before it's further processed.

Based on the WordPress plugins library, the WP Time Capsule plugin is active on 20,000+ websites.

Timeline

- **07-01-2020** – Reported the vulnerabilities to the developer of both plugins.
- **07-01-2020** – Released protection module to all Patchstack (formerly WebARX) customers.
- **08-01-2020** – Developer of the plugin released a new version for both plugins.
- **14-01-2020** – Security advisory publicly released.

Start listening

Related Articles

View All >

WORDPRESS SECURITY VULNERABILITIES

Most Common WordPress Plugin Vulnerabilities & How to Fix Them

LAST PATCH, WORDPRESS PLUGIN SECURITY

Patching an Arbitrary User Creation Security Bug in "thecartpress" Plugin

PATCHSTACK WEEKLY

Patchstack Weekly #51: How One Vulnerability Affects Many

Patchstack

About us

Careers

Media kit

Articles & insight

Whitepaper 2021

Social

LinkedIn

Facebook

Twitter

hackuu

Join Discord

DPA Privacy Policy Terms & Conditions