Ram Gall May 18, 2022

Critical Privilege Escalation Vulnerability in Jupiter and JupiterX Premium Themes

On April 5, 2022, the Wordfence Threat Intelligence team initiated the responsible disclosure process for a set of vulnerabilities in the Jupiter and JupiterX Premium themes and the required JupiterX Core companion plugin for WordPress, which included a critical privilege escalation vulnerability that allowed any user to become an administrat

The plugin developers quickly replied and we sent over the full disclosure on the same day. Fully patched versions of vulnerable components were made available on May 10, 2022.

Wordfence Premium, Wordfence Care, and Wordfence Response customers received a firewall rule protecting agains these vulnerabilities on April 5, 2022. Sites still running the free version of Wordfence received the same protection 3(days later, on May 4, 2022.

We strongly recommend updating to the latest patched version for your installation as soon as possible, since this w remove the vulnerabilities. If you are using the classic Jupiter theme, you should update to at least version 6.10.2. If are using the JupiterX theme, you should update to at least version 2.0.8 of the JupiterX Core plugin, and at least ver 2.0.7 of the JupiterX Core theme, which are the latest versions available at the time of this writing.

Description: Authenticated Privilege Escalation and Post deletion
Affected Software: Jupiter Theme and JupiterX Core Plugin
Slug(s): jupiter (theme), jupiterx-core(plugin)
Developer: ArtBees
Affected Versions: Jupiter Theme <= 6.10.1 and JupiterX Core Plugin <= 2.0.7
CVE ID: CVE-2022-1654
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
Researcher(s): Ramuel Gall
Fully Patched Versions: Jupiter Theme 6.10.2 and JupiterX Core Plugin 2.0.8

This vulnerability allows any authenticated attacker, including a subscriber or customer-level attacker, to gain administrative privileges and completely take over any site running either the Jupiter Theme or JupiterX Core Plugin

The classic Jupiter Theme contains a function, `uninstallTemplate`, which is intended to reset a site after a template uninstalled, but has the additional effect of elevating the user calling the function to an administrator role. In JupiterX this functionality has been migrated to the JupiterX Core plugin. Vulnerable versions register AJAX actions but do not perform any capability checks or nonce checks.

On a site with a vulnerable version of the Jupiter Theme installed, any logged-in user can elevate their privileges to the of an administrator by sending an AJAX request with the `action` parameter set to `abb_uninstall_template`. This ca the `uninstallTemplate` function, which calls the `resetWordpressDatabase` function, where the site is effectively reinstalled with the currently logged-in user as the new site owner.

On a site where a vulnerable version of the JupiterX Core plugin is installed, the same functionality can also be acces by sending an AJAX request with the `action` parameter set to `jupiterx_core_cp_uninstall_template`.

Description: Insufficient Access Control leading to Authenticated Arbitrary Plugin Deactivation and Settings Modification
Affected Software: JupiterX Theme and JupiterX Core Plugin
Slug(s): jupiterx (theme), jupiterx-core(plugin)
Developer: ArtBees
Affected Versions: JupiterX Theme <= 2.0.6 and JupiterX Core <= 2.0.6
CVE ID: CVE-2022-1656
CVSS score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
Researcher(s): Ramuel Gall
Fully Patched Versions: JupiterX Theme 2.0.7 and JupiterX Core Plugin 2.0.7

This vulnerability allows an attacker to reduce site security or damage functionality.

Vulnerable versions of the JupiterX Theme allow any logged-in user, including subscriber-level users, to access any o the functions registered in `lib/api/api/ajax.php`, which also grant access to the `jupiterx_api_ajax_` actions registered by the JupiterX Core Plugin. This includes the ability to deactivate arbitrary plugins as well as update the theme's API key.

Description: Authenticated Path Traversal and Local File Inclusion
Affected Software: JupiterX Theme and Jupiter Theme
Slug(s): jupiterx (theme), jupiter(theme)
Developer: ArtBees
Affected Versions: JupiterX Theme <= 2.0.6 and Jupiter Theme <= 6.10.1
CVE ID: CVE-2022-1657
CVSS score: 8.1 (High)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:N
Researcher(s): Ramuel Gall
Fully Patched Versions: JupiterX Theme 2.0.7 and Jupiter Theme 6.10.2

This vulnerability could allow an attacker to obtain privileged information, such as nonce values, or perform restricted actions, by including and executing files from any location on the site.

Vulnerable versions of the Jupiter and JupiterX Themes allow logged-in users, including subscriber-level users, to perform Path Traversal and Local File inclusion. In the JupiterX theme, the `jupiterx_cp_load_pane_action` AJAX action present in the `lib/admin/control-panel/control-panel.php` file calls the `load_control_panel_pane` function. It is possible to use this action to include any local PHP file via the `slug` parameter. The Jupiter theme has a nearly identical vulnerability which can be exploited via the `mka_cp_load_pane_action` AJAX action present in the `framework/admin/control-panel/logic/functions.php` file, which calls the `mka_cp_load_pane_action` function.

Description: Insufficient Access Control leading to Authenticated Arbitrary Plugin Deletion
Affected Software: Jupiter Theme
Slug(s): jupiter (theme)
Developer: ArtBees
Affected Versions: Jupiter Theme <= 6.10.1
CVE ID: CVE-2022-1658
CVSS score: 6.5 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:N/I:H/A:N
Researcher(s): Ramuel Gall
Fully Patched Versions: Jupiter Theme 6.10.2

This vulnerability allows an attacker to reduce site security or damage functionality.

Vulnerable versions of the Jupiter Theme allow arbitrary plugin deletion by any authenticated user, including users wi

on the site.

Description: Information Disclosure, Modification, and Denial of Service
Affected Software: JupiterX Core Plugin
Slug(s): jupiterx-core (plugin)
Developer: ArtBees
Affected Versions: JupiterX Core Plugin <= 2.0.6
CVE ID: CVE-2022-1659
CVSS score: 6.3 (Medium)
CVSS Vector: CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:L/I:L/A:L
Researcher(s): Ramuel Gall
Fully Patched Versions: JupiterX Core Plugin 2.0.7

This vulnerability allows an attacker to view site configuration and logged-in users, modify post conditions, or perforr denial of service attack.

Vulnerable versions of the JupiterX Core plugin register an AJAX action `jupiterx_conditional_manager` which can used to call any function in the `includes/condition/class-condition-manager.php` file by sending the desired function to call in the `sub_action` parameter.

Timeline

April 5, 2022 – The Wordfence Threat Intelligence team finishes our investigation of the Jupiter and JupiterX Theme: We release a firewall rule to protect Wordfence Premium, Wordfence Care, and Wordfence Response customers. We contact the theme developer and send over the full disclosure.
April 28, 2022 – A partially patched version of the JupiterX theme and JupiterX Core plugin is released.
May 3, 2022 – We follow up with the theme developer about additional patches and notify them of an additional vulnerability we found in the Jupiter Theme.
May 4, 2022 – Firewall rule becomes available to Wordfence free users.
May 10, 2022 – Fully Patched versions of the Jupiter Theme and JupiterX Core plugin are released. We verify that all vulnerabilities are addressed.

Conclusion

In today's article, we covered a number of vulnerabilities present in the Jupiter and JupiterX themes and the JupiterX Core companion plugin. The most severe vulnerability allows any logged-in user to easily gain administrator privilege

Wordfence Premium, Wordfence Care, and Wordfence Response customers have been protected from these vulnerabilities since April 5, 2022, and free Wordfence users received the same protection on May 4, 2022.

We strongly recommend updating to the latest versions of the impacted themes and plugins available immediately.

Since several versions across several slugs are impacted, we'll reiterate what you should update:

If you are running the **Jupiter Theme** version **6.10.1** or below, you should immediately update to version **6.10.2** or hig

If you are running the **JupiterX Theme** version **2.0.6** or below, you should immediately update to version **2.0.7** or high

If you are running the **JupiterX Core Plugin** version **2.0.7** or below, you should immediately update it to version **2.0.8** higher.

If you know anyone using the Jupiter theme or the JupiterX theme, we urge you to forward this advisory to them as t most severe vulnerability allows complete site takeover.

If you believe your site has been compromised as a result of this vulnerability or any other vulnerability, we offer Incid Response services via Wordfence Care. If you need your site cleaned immediately, Wordfence Response offers the same service with 24/7/365 availability and a 1-hour response time. Both these products include hands-on support i case you need further assistance.

Comments

Breaking WordPress Security Research in your inbox as it happens.

you@example.com

By checking this box I agree to the terms of service and privacy policy.*

SIGN UP

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.

Stay Updated

Sign up for news and updates from our panel of experienced security professionals.

you@example.com

By checking this box I agree to the terms of service and privacy policy.*

SIGN UP