Subject: A Critical Security Flaw in the miniOrange Social Login and Register Plugin
Posted by admin on Thu, 30 Jul 2026 08:06:47 GMT
View Forum Message <> Reply to Message

A Critical Security Flaw in the miniOrange Social Login and Register Plugin

"How to protect your WordPress site from the miniOrange Social Login and Register security flaw."

Meta Description: Critical security flaw in miniOrange Social Login and Register plugin allows attackers to gain access to any user account. Update to latest version to protect your site.

miniOrange-Social-Login

Jul 2, 2023

A critical security flaw has been found in the miniOrange Social Login and Register plugin, which is a popular WordPress plugin that allows users to log in to WordPress sites using their social media accounts, such as Facebook, Twitter, and Google.

The flaw, which has been tracked as CVE-2023-2982, allows attackers to gain access to any user account on a site, including those used to administer the site. The flaw is caused by the fact that the encryption key used to secure the information during login using social media accounts is hard-coded. This means that an attacker who knows the email address of a user account can create a valid request with a properly encrypted email address used to identify the user.

Once an attacker has gained access to a user account, they can then do whatever they want with the account, including changing the password, deleting the account, or accessing any sensitive data that is stored in the account.

The flaw was discovered by Wordfence researcher István Márton and has been patched in the latest version of the miniOrange Social Login and Register plugin (version 7.6.5). However, many websites are still running older versions of the plugin, which are vulnerable to the attack.
How to Protect Yourself

If you are using the miniOrange Social Login and Register plugin, you should update to the latest version as soon as possible. You can also check if your website is vulnerable to the attack by using the Wordfence scanner: https://www.wordfence.com/.

In addition to updating your plugins, there are a few other things you can do to protect your WordPress site from security flaws:

Keep your WordPress core software up to date.

Use a security plugin, such as Wordfence.

Monitor your website for suspicious activity.

Back up your website regularly.

By following these tips, you can help to keep your WordPress site safe from attack.

The Impact of This Flaw

This is a serious security flaw that could have a significant impact on any website that is using the miniOrange Social Login and Register plugin. If an attacker is able to exploit this flaw, they could gain access to any user account on the site, including those used to administer the site. This could allow them to do anything they want with the site, including changing the content, deleting user accounts, or even taking the site offline.

How to Stay Informed

To stay informed about security flaws in WordPress plugins, you can subscribe to the Wordfence blog or follow Wordfence on Twitter. You can also check the WordPress Plugin Directory for security advisories.

Conclusion

This is a serious security flaw that should be taken seriously by anyone who is using the miniOrange Social Login and Register plugin. If you are using this plugin, it is important to update to the latest version as soon as possible to protect your website from attack. By following the tips in this article, you can help to keep your WordPress site safe from attack.

Extra Tags:

How to protect your WordPress site from the miniOrange Social Login and Register security flaw

How to update the miniOrange Social Login and Register plugin to the latest version

How to check if your WordPress site is vulnerable to the miniOrange Social Login and Register security flaw

What is the impact of the miniOrange Social Login and Register security flaw?

How to stay informed about security flaws in WordPress plugins

miniOrange Social Login and Register plugin