

Date: February 3, 2022

WORDPRESS PLUGIN EXPOSES HALF A MILLION SITES TO ATTACK

1. 13.7 MILLION ATTACKS IN 36 HOURS SEEN FROM MORE THAN 16,000 DIFFERENT IP ADDRESSES



A massive wave of ongoing attacks against more than 1.6 million WordPress sites has been identified by researchers. Users told to update Essential Addons for Elementor WordPress plugin immediately. A popular WordPress plugin used by more than a million websites all over the world has been found to be carrying a critical remote code execution flaw that allowed potential malicious actors to perform a local file inclusion attack.

- i. They report seeing more than 13.7 million different attack attempts over a 36-hour period, all of which focus on exploiting four different WordPress plug-ins and several Epsilon framework themes.
- ii. Due to the severity of these vulnerabilities and the massive campaign targeting them, it is incredibly important to ensure your site is protected from compromise.
- iii. The excellent news is that the plugins' house owners are fast to react, when the vulnerabilities are disclosed. Site owners working WordPress are suggested to maintain all of their addons up to date always, to convey the chance of an assault right down to a minimal.

2. CALL TO ACTION

- I. We recommend that all sites be updated to the latest, patched versions of the plug-ins and themes. WordPress plug-ins continue to be a major risk to any web application, making them a regular target for attackers.
- II. We strongly recommend ensuring that any sites running one of these plug-ins or themes has been updated to the patched version. Simply updating the plug-ins and themes will ensure that your site stays safe from compromise against any exploits targeting these vulnerabilities.
- III. Website owners/developers need to be vigilant about third-party plug-ins and frameworks and stay on top of security updates. Websites can be secured using web application firewalls, as well as client-side visibility solutions that can reveal the presence of malicious code on their sites
- IV. For all WordPress site owners, if your site is using Elementor, make it your priority to get things updated today to avoid your website security being compromised.
- V. Those running Essential Addons for Elementor have two ways to go about fixing the issue: either downloading the latest version from this link, or heading over to the WordPress dashboard and triggering the update directly from there.

We are committed to helping our clients not only understand but respond quickly to this situation. If you need any help – please reach out to us at info@net-square.com.

About us:

Net Square is a technology-based security services organization. Our focus is on the security of our client's network and applications. Net Square undertakes vanilla Vulnerability and Penetration Testing Services with its unique model of "No Stone Left Unturned". With a team of security experts, we are able to help some of the best logos globally manage their cyber security risk effectively. In this time of limited skill set and high cost, we are able to provide high-quality service at a cost that balances the business value with the associated security concerns. Our thoroughly researched methodologies and our knowledge of the latest attacks vectors help us in providing our clients insights into the gaps in the security posture of their applications and network.