The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
https://www.cisa.gov/tlp
Sources may use TLP:WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

DATE(S) ISSUED:
01/21/2022

SUBJECT:
A Backdoor in WordPress AccessPress Plugins and Themes Could Allow an Attacker Access to a Targeted Website

OVERVIEW:
A backdoor has been discovered in WordPress AccessPress plugins and themes, which could allow an attacker access to a targeted website. AccessPress plugins and themes are used to provide website functionality and design options to website administrators. Successful exploitation of this backdoor could allow an attacker to redirect users to malicious sites as well as access to the vulnerable website.

THREAT INTELLIGENCE:
There are currently reports of websites redirecting users to malicious sites.

The references for this state that malicious actors have been compromising affected sites with backdoors as far back as September 2021.

SYSTEMS AFFECTED:
- accesspress-anonymous-post 2.8.0
- accesspress-custom-css 2.0.1
- accesspress-custom-post-type 1.0.8
- accesspress-facebook-auto-post 2.1.3
- accesspress-instagram-feed 4.0.3
- accesspress-pinterest 3.3.3
- accesspress-social-counter 1.9.1
- accesspress-social-icons 1.8.2
- accesspress-social-login-lite 3.4.7
- accesspress-social-share 4.5.5
- accesspress-twitter-auto-post 1.4.5
- accesspress-twitter-feed 1.6.7
- ak-menu-icons-lite 1.0.9
- ap-companion 1.0.7
- ap-contact-form 1.0.6
- ap-custom-testimonial 1.4.6
- ap-mega-menu 3.0.5

- ap-pricing-tables-lite 1.1.2
- apex-notification-bar-lite 2.0.4
- cf7-store-to-db-lite 1.0.9
- comments-disable-accesspress 1.0.7
- easy-side-tab-cta 1.0.7
- everest-admin-theme-lite 1.0.7
- everest-coming-soon-lite 1.1.0
- everest-comment-rating-lite 2.0.4
- everest-counter-lite 2.0.7
- everest-faq-manager-lite 1.0.8
- everest-gallery-lite 1.0.8
- everest-google-places-reviews-lite 1.0.9
- everest-review-lite 1.0.7
- everest-tab-lite 2.0.3
- everest-timeline-lite 1.1.1
- inline-call-to-action-builder-lit 1.1.0
- product-slider-for-woocommerce-lite 1.1.5
- smart-logo-showcase-lite 1.1.7
- smart-scroll-posts 2.0.8
- smart-scroll-to-top-lite 1.0.3
- total-gdpr-compliance-lite 1.0.4
- total-team-lite 1.1.1
- ultimate-author-box-lite 1.1.2
- ultimate-form-builder-lite 1.5.0
- woo-badge-designer-lite 1.1.0
- wp-1-slider 1.2.9
- wp-blog-manager-lite 1.1.0
- wp-comment-designer-lite 2.0.3
- wp-cookie-user-info 1.0.7
- wp-facebook-review-showcase-lite 1.0.9
- wp-fb-messenger-button-lite 2.0.7
- wp-floating-menu 1.4.4
- wp-media-manager-lite 1.1.2
- wp-popup-banners 1.2.3
- wp-popup-lite 1.0.8
- wp-product-gallery-lite 1.1.1
- accessbuddy 1.0.0
- accesspress-basic 3.2.1
- accesspress-lite 2.92
- accesspress-mag 2.6.5
- accesspress-parallax 4.5
- accesspress-ray 1.19.5
- accesspress-root 2.5
- accesspress-staple 1.9.1
- accesspress-store 2.4.9
- agency-lite 1.1.6
- aplite 1.0.6
- bingle 1.0.4

- bloger 1.2.6
- construction-lite 1.2.5
- doko 1.0.27
- enlighten 1.3.5
- fashstore 1.2.1
- fotography 2.4.0
- gaga-corp 1.0.8
- gaga-lite 1.4.2
- one-paze 2.2.8
- parallax-blog 3.1.1574941215
- parallaxsome 1.3.6
- punte 1.1.2
- revolve 1.3.1
- ripple 1.2.0
- scrollme 2.1.0
- sportsmag 1.2.1
- storevilla 1.4.1
- swing-lite 1.1.9
- the-launcher 1.3.2
- the-Monday 1.4.1
- uncode-lite 1.3.1
- unicon-lite 1.2.6
- vmag 1.2.7
- vmagazine-lite 1.3.5
- vmagazine-news 1.0.5
- zigcy-baby 1.0.6
- zigcy-cosmetics 1.0.5
- zigcy-lite 2.0.9

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
A backdoor has been discovered in WordPress AccessPress plugins and themes, which could allow an attacker access to a targeted website. When the compromised plugin or theme is installed, a payload is deployed that creates a webshell into "./wp-includes/vars.php" and then hides its tracks by deleting its files. When successfully installed, the backdoor gives the threat actor control over the infected website.

RECOMMENDATIONS:
We recommend the following actions be taken:
- Consult the list of affected themes and plugins provided in the Systems Affected section above and verify if you are utilizing any of them in your environment.

- Update all affected plugins and themes to their newest safe version, published by AccessPress.
- If an affected plugin or theme was found to be in use, check all web sites and servers for signs of potential compromise.
    - BleepingComputer provided an extensive list of checks that can be used to determine if a site may have been compromised. Information can be found at the reference below in the “Am I affected?” section near the bottom of the article.

REFERENCES:

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-24867

Jetpack:
https://jetpack.com/2022/01/18/backdoor-found-in-themes-and-plugins-from-accesspress-themes/

BleepingComputer:
https://www.bleepingcomputer.com/news/security/over-90-wordpress-themes-plugins-backdoored-in-supply-chain-attack/

Sucuri Blog:
https://blog.sucuri.net/2022/01/accesspress-themes-hit-with-targeted-supply-chain-attack.html