info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 0009

## ADVERTISING PLUG-IN ON WORDPRESS SITES

**DATE ISSUED:** 9th July 2020

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | HIGH |
| EASE OF EXPLOIT | LOW | MEDIUM | HIGH |

## OVERVIEW

Premium advertising plugin Adning on Wordpress sites contains critical vulnerabilities allowing remote-code execution by unauthorised users facilitation full takeover of websites, but at this stage attacks have been limited in scope and scale.

## BREAKDOWN

Visitors to Wordpress sites using the Adning plugin to display banners were able to access the AJAX action '_ning_upload_image' with a 'nopriv_hook' without being logged in as a legitimate user enabling the supply of allowed file types facilitating the upload of malware through compressed files. This function provides no capability check or nonce check allowing for path traversal. If an attacker were able to use the '_ning_remove_image' function call, this provided the potential to wipe the site and upload their own content

## REMEDIATION STEPS

- Deploy new version v1.5.6 of the Adning plugin which includes relevant security patches

## REFERENCES & RESOURCES

Threatpost: https://threatpost.com/advertising-plugin-wordpress-full-site-takeovers/157283/
Adning http://adning.com/