UNISPHERE SOLUTIONS
info@unisphere.co.nz
www.unisphere.co.nz

# CYBER GUIDANCE ISSUE 00065

## WORDPRESS FLAWED UPDATES

**DATE ISSUED:** 10th November 2020

| | | | |
|---|---|---|---|
| IMPACT | LOW | MEDIUM | **HIGH** |
| EASE OF EXPLOIT | HARD | **MEDIUM** | EASY |

## OVERVIEW

WordPress released a critical security update 5.5.2 which was closely followed by 5.5.3 the next day after a number of flaws were found in 5.5.2.

## BREAKDOWN

Auto-updates of 5.5.2 accidentally pushed updates on 455million users that disabled new WordPress installs and was immediately halted following this realisation. Some customers inadvertently received a pre-release Alpha version of 5.5.3 download while WordPress attempted to restrict the download of 5.5.2 in an effort to stem the spread of the issues in this version that broke administration pages and prevented new installs. This highlights concerns regarding the auto-update feature and lack of control presented by this case and the potential for rogue updates by malicious actors to be pushed out to users.

## REMEDIATION STEPS

- Any users who received the pre-release alpha update must revert to version 5.5.2 in order to install the fully functional 5.5.3 version
- Update all WordPress sites to version 5.5.3 to apply security patches and receive full functionality by visiting Dashboard > Updates

## REFERENCES & RESOURCES

Threatpost https://threatpost.com/wordpress-flawed-security-updates/160849/
WordPress https://wordpress.org/support/topic/wordpress-5-5-3-alpha-auto-updates/