National Computer Board

Computer Emergency Response Team of Mauritius

(CERT-MU)

CERT-MU

Targeted Security Alert

WordPress Stores Cross-Site Scripting (XSS) Vulnerability

Original Issue Date: May 04, 2015

Severity Rating: High

System Affected:

- WordPress 4.2 and prior versions

Description:

Current versions of WordPress are vulnerable to a stored XSS. An unauthenticated attacker can inject JavaScript in WordPress comments. The script is triggered when the comment is viewed.

If triggered by a logged-in administrator, under default settings the attacker can leverage the vulnerability to execute arbitrary code on the server via the plugin and theme editors.

Alternatively the attacker could change the administrator's password, create new administrator accounts, or do whatever else the currently logged-in administrator can do on the target system.

Solution:

Download WordPress 4.2.1 or venture over to Dashboard → Updates and simply click "Update Now".

References

WordPress

https://wordpress.org/news/2015/04/wordpress-4-2-1/

Komodo Consulting

http://www.komodosec.com/wordpress_stored_xss/?utm_source=CERT%27s&utm_campaign=957d23cdd0-CYSNIFF_Alert_29_4_2015&utm_medium=email&utm_term=0_65b9bb9fd2-957d23cdd0-281438965

For more information please contact CERT-MU team on:

Hotline No: (+230) 800 2378

Fax No: (+230) 208 0119

Gen. Info. : contact@cert.ncb.mu

Incident: incident@cert.ncb.mu

Website: www.cert-mu.org.mu