Advisory Alert

Alert No : AAA170825 Date : 25-Aug-17 13:38 PM

Security Updates for 25th August 2017

Overview			
	High	Postgresql	▪ Gain Unauthorized Access
	Medium and Low	Fortinet	▪ Arbitrary Code Execution
		WebSphere	▪ Weaker than Expected Security
		WordPress	▪ Cross-Site Scripting Attack

Description / Impact

Postgresql	• A vulnerability in Postgresql to incorrect authentication flaw allowing remote attackers to gain access to the database accounts with an empty password. • Affected Systems: **Version before 9.2.22, 9.3.18, 9.4.13, 9.5.8 & 9.6.4** • Officially Acknowledged by the Vendor: **Yes**
Fortinet	• A vulnerability in the Fortinet FortiManager allows remote authenticated users to inject arbitrary web scripts or HTML. • Affected Systems: **V5.2.1 and earlier & v5.0.10 and earlier** • Officially Acknowledged by the Vendor: **Yes**
WebSphere	• A vulnerability in the IBM WebSphere Application Server could provide weaker than expected security after using the Admin console to update the web services security bindings settings. • Affected Systems: **Version 8.0, 8.5 & 9.0** • Officially Acknowledged by the Vendor: **Yes**
WordPress	• A Cross-site scripting (XSS) vulnerability exits in the WordPress admin panel when the Broken Link Checker plugin is installed. • Affected Systems: **Before 1.10.9** • Officially Acknowledged by the Vendor: **Yes**

Risk Reduction Recommendations

Visit the links below and follow the instructions given by respective vendors.

Postgresql	https://www.postgresql.org/about/news/1772/
WordPress	https://wordpress.org/plugins/broken-link-checker/#developers
Fortinet	https://fortiguard.com/psirt/FG-IR-15-011
WebSphere	http://www-01.ibm.com/support/docview.wss?uid=swg22006810

Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind.

Financial Sector Computer Security Incident Response Team, Sri Lanka
Hotline: + 94 112039777
Report incident to incident@fincsirt.lk