Advisory Alert

Alert No : AAA170227 Date : 27-Feb-17 10:18 AM

Security Updates for 27th February 2017

Overview

High	Wireshark	▪	Exhaust System Memory
	Linux	▪	Denial of Service
	Nagios	▪	Bypass System security
Medium and Low	Wordpress	▪	Reflected XSS
	Websphere	▪	Cross-Site Scripting

Description / Impact

Wireshark	• A vulnerability in the Wireshark 2.2.4 and earlier allows attackers to Exhaust System Memory via crafted or malformed capture file.
Linux	• A vulnerability in the Linux kernel before 4.9.7 allows local users to cause a denial of service attack.
Nagios	• A vulnerability in the Nagios 4.2.4 and earlier allows local users to gain root privileges via a hard link attack on the Nagios init script file.
Wordpress	• A vulnerability in the WP Mail plugin before 1.2 for WordPress, allows for a reflected XSS attack.
Websphere	• A vulnerability in the IBM WebSphere Application Server 7.0, 8.0, and 9.0 is vulnerable to cross-site scripting.

Risk Reduction Recommendations

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

Wireshark	https://nvd.nist.gov/nvd.cfm?cvename=CVE-2017-6014
Linux	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-5576
Nagios	http://www.openwall.com/lists/oss-security/2016/12/30/6
Wordpress	https://nvd.nist.gov/nvd.cfm?cvename=CVE-2017-5942
Websphere	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2017-1121

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