Advisory Alert

Alert No: AAA180104 Date: 04-Jan-18 12:56 PM

Security Updates for 04th January 2018

Overview		
High	Multiple CPU Architectures phpMyAdmin	▪ Side-Channel Attack ▪ Cross-Site Request Forgery Attack
Medium and Low	Linux	▪ Multiple Vulnerabilities
Description / Impact		
Multiple CPU Architectures	• CPU hardware implementations are vulnerable to side-channel attacks. An attacker could execute arbitrary code with user privileges to gain access to sensitive information. • Affected Vendors: **Arm, Intel, AMD *(Confirmed at this moment)** • Officially Acknowledged by the Vendors: **Yes**	
phpMyAdmin	• phpMyAdmin is vulnerable to Cross-Site Request Forgery Attack. A remote attacker can deceive a user to click on a crafted URL and perform harmful database operations. (e.g. Deleting records) • Affected Systems: **phpMyAdmin 4.7.x (prior to 4.7.7)** • Officially Acknowledged by the Vendor: **Yes**	
Linux	• Several vulnerabilities have been discovered in the Linux Kernel that may lead to a privilege escalation, denial of service attack or sensitive information disclosure. • Affected Systems: **Linux kernel through 4.14.3, 4.13.11, 4.14.8, 4.14.4, 4.14.5, 4.14.6, 4.14.7, 4.14.8, 2.6.32 and later.** • Officially Acknowledged by the Vendor: **Yes**	
Risk Reduction Recommendations	**Visit the links below and follow the instructions given by respective vendors.**	
Multiple CPU Architectures	1. https://www.kb.cert.org/vuls/id/584653 2. https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV180002 3. https://access.redhat.com/security/vulnerabilities/speculativeexecution 4. https://googleprojectzero.blogspot.com/2018/01/reading-privileged-memory-with-side.html	
phpMyAdmin	https://www.phpmyadmin.net/security/PMASA-2017-9/	
Linux	https://www.debian.org/security/2017/dsa-4073	
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