Advisory Alert

Alert No : AAA030217 Date : 03-Feb-17 10:12 AM

Security Updates for 03rd February 2017

Overview	High	Joomla	▪ Bypass security constraint
		PHP	▪ Denial of Service
		PHP pecl	▪ Execute Arbitrary Commands
	Medium and Low	Cisco	▪ Bypass security constraint

Description / Impact

Joomla	• A vulnerability in the Joomla 3.4.4 through 3.6.3 allows attackers to reset username, password, and user group assignments and possibly perform other user account modifications.
PHP	• Multiple vulnerabilities in PHP before 5.6.30 and 7.0.x before 7.0.15 allows remote attackers to cause a denial of service attack.
PHP pecl	• A vulnerability in the php pecl_http before 3.0.1 might allow remote attackers to execute arbitrary code.
Cisco	• A vulnerability in the content scanning engine of Cisco AsyncOS Software for Cisco Email Security Appliances (ESA) could allow an unauthenticated, remote attacker to bypass configured message or content filters on the device.

Risk Reduction Recommendations

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

Joomla	https://developer.joomla.org/security-centre/661-20161003-core-account-modifications.html
PHP	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10160 , https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-10158
PHP pecl	http://www.openwall.com/lists/oss-security/2016/06/29/4
Cisco	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170118-esa

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