Advisory Alert

Alert No : AAA170609 Date : 09-Jun-17 12:42 PM

Security Updates for 9th June 2017

Overview		
High	Cisco Prime Cisco AnyConnect	▪ Remote Code Execution ▪ Local Privilege Escalation
Medium and Low	Tomcat	▪ Bypass Security Restrictions
Description / Impact		
Cisco Prime	• A vulnerability in the role-based access control of Cisco Prime Data Center Network could allow remote attackers to access sensitive information or execute arbitrary code. • Affected Systems: **Data Center Network Manager version 10.1(2)** • Officially Acknowledged by the Vendor: **Yes**	
Cisco AnyConnect	• A vulnerability in the Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker run an executable file with privilege equivalent to the Microsoft Windows SYSTEM account. • Affected Systems: **Versions prior to 4.4.02034** • Officially Acknowledged by the Vendor: **Yes**	
Apache Tomcat	• A vulnerability in the Apache Tomcat 7, 8.0 & 9 may allow remote attackers to bypass the security restrictions. • Affected Systems: **Apache Tomcat 7, 8.0 & 9** • Officially Acknowledged by the Vendor: **Yes**	
Risk Reduction Recommendations	**Visit the links below and follow the instructions given by respective vendors.**	
Cisco Prime	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-dcnm1	
Cisco AnyConnect	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20170607-anyconnect	
Apache Tomcat	http://tomcat.apache.org/security-9.html#Fixed_in_Apache_Tomcat_9.0.0.M21	
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