Advisory Alert

Alert No: AAB180130 Date: 30-Jan-18 9:38 AM

Security Updates for 30th January 2018

Overview	High	Cisco cURL	▪ Remote Code Execution & Denial of Service Attack ▪ Sensitive Information Disclosure
Description / Impact	Cisco ASA	• A vulnerability in Cisco Adaptive Security Appliance could allow an unauthenticated, remote attacker to execute arbitrary code and cause a denial of service attack. • Affected Products: **3000 Series Industrial Security Appliance (ISA), ASA 5500 Series Adaptive Security Appliances, ASA 5500-X Series Next-Generation Firewalls, ASA Services Module for Cisco Catalyst 6500 Series Switches and Cisco 7600 Series Routers, ASA 1000V Cloud Firewall, Adaptive Security Virtual Appliance (ASAv), Firepower 2100 Series Security Appliance, Firepower 4110 Security Appliance, Firepower 9300 ASA Security Module, Firepower Threat Defense Software (FTD)** • Officially Acknowledged by the Vendor: **Yes**	
	cURL libcurl	• A vulnerability in cURL libcurl could allow a remote attacker to obtain sensitive information. • Affected Systems: **cURL libcurl 7.1 - 7.57.0** • Officially Acknowledged by the Vendor: **Yes**	
Risk Reduction Recommendations	**Visit the links below and follow the instructions given by respective vendors.** Cisco ASA https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180129-asa1 cURL libcurl https://curl.haxx.se/docs/adv_2018-b3bf.html		
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