Vulnerability Alert

Alert No: AVA180405

Date: 05-Apr-18 12:16 PM

Cisco Vulnerability: Remote Code Execution

Overview	**Critical vulnerability in Cisco IOS Software and Cisco IOS XE Software. (CVE-2018-0171)**
Description / Impact	• A vulnerability in the Cisco Smart Install Client code allows an authenticated attacker to execute remote arbitrary code and get full control over a vulnerable device. • Cisco released a patch update to address the vulnerability which has been given a base Common Vulnerability Score System (CVSS) score of **9.8 (Critical)** • It is reported that approximately 250,000 unpatched devices are open to be exploited. • Some of the vulnerable devices (But not limited) are mentioned below
Risk Reduction Recommendations	**Immediate Actions to be taken:** 1. Please contact the Cisco Partner to get the relevant patch update.
References	1. https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2 2. https://embedi.com/blog/cisco-smart-install-remote-code-execution/
Disclaimer	**The information provided herein is on "as is" basis, without warranty of any kind.**

Catalyst	**4500 Supervisor Engines, 3850 Series, 3750 Series, 3650 Series, 3560 Series, 2960 Series, 2975 Series**
IE	**2000, 3000, 3010, 4000, 4010, 5000**
SM-ES2 SKUs, SM-X-ES3 SKUs	
NME-16ES-1G-P	

Financial Sector Computer Security Incident Response Team, Sri Lanka
Hotline: + 94 112039777
Report incident to incident@fincsirt.lk