



MINISTRY OF
HOME AFFAIRS
CAYMAN ISLANDS GOVERNMENT

National Cyber Awareness System:

[Cisco Releases Security Updates](#)

04/06/2016

Original release date: April 06, 2016

Cisco has released security updates to address vulnerabilities in multiple products. Exploitation of some of these vulnerabilities could allow a remote attacker to take control of an affected system.

Users and administrators are encouraged to review the following Cisco Security Advisories and apply the necessary updates:

- [cisco-sa-20160406-privauth](#): Cisco Prime Infrastructure and Evolved Programmable Network Manager Privilege Escalation API Vulnerability
- [cisco-sa-20160406-cts1](#): Cisco TelePresence Server Crafted URL Handling Denial-of-Service Vulnerability
- [cisco-sa-20160406-ucs](#): Cisco UCS Invicta Default SSH Key Vulnerability
- [cisco-sa-20160406-cts](#): Cisco TelePresence Server Crafted Ipv6 Packet Handling Denial-of-Service Vulnerability
- [cisco-sa-20160406-remcode](#): Cisco Prime Infrastructure and Evolved Programmable Network Manager Remote Code Execution Vulnerability
- [cisco-sa-20160406-cts2](#): Cisco TelePresence Server Malformed STUN Packet Processing Denial-of-Service Vulnerability

Source: US-CERT

Stay connected with the Ministry of Home Affairs for information concerning national security and public safety.

