

Cisco Multiple Vulnerabilities Security Updates October 2018

Cisco has issued updates to address vulnerabilities affecting multiple products that could be exploited by remote attacker thereby enabling the attacker to gain full access to an affected system.

CERT.NG encourages users and administrators to review Cisco Security Advisories and the necessary updates should be applied:

- Cisco Stealthwatch Management Console Authentication Bypass Vulnerability [cisco-sa-20181107-smc-auth-bypass](https://www.cisco.com/cisco-sa-20181107-smc-auth-bypass)
- Cisco Unity Express Arbitrary Command Execution Vulnerability [cisco-sa-20181107-cue](https://www.cisco.com/cisco-sa-20181107-cue)
- Cisco Meraki Local Status Page Privilege Escalation Vulnerability [cisco-sa-20181107-meraki](https://www.cisco.com/cisco-sa-20181107-meraki)



www.cerrt.ng

support@cerrt.ng

Telephone line; (+234)-0800998877665544.