UGANDA NATIONAL COMPUTER EMERGENCY RESPONSE TEAM AND COORDINATION CENTER (CERT.UG/CC)

3/29/2018

CISCO XE VULNERABILITY

Severity: CERT.UG rates the severity of this vulnerability as **CRITICAL**.

Risk Assessment: Cisco has released updates to address vulnerabilities affecting multiple products. A remote attacker could exploit some of these vulnerabilities to take control of an affected system. A vulnerability in Cisco IOS XE Software could allow an unauthenticated, remote attacker to log in to a device running an affected release of Cisco IOS XE Software with the default username and password that are used at initial boot. The vulnerability is due to an undocumented user account with privilege level 15 that has a default username and password. An attacker could exploit this vulnerability by using this account to remotely connect to an affected device. A successful exploit could allow the attacker to log in to the device with privilege level 15 access.

- **Risk Mitigation:** CERT.UG encourages users and administrators to review the following Cisco Security Advisories and apply the necessary updates:
    - Cisco IOS XE Software Static Credential Vulnerability cisco-sa-20180328-xesc (link is external)
    - Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability cisco-sa-20180328-smi2 (link is external)
    - Cisco IOS and IOS XE Software Quality of Service Remote Code Execution Vulnerability cisco-sa-20180328-qos