Advanced Notification of Cyber Threats against Cisco Nexus 9000 Series Switches SSH Key Vulnerability

Security Advisory	ADV-19-14	**Criticality**	Critical	
Advisory Released On	7 May 2019			

Impact

A vulnerability in Cisco Nexus 9000 Mode Switch Software that could be exploited to gain remote access with root user privileges.

Solution

Adhere the advices written under the recommendations section.

Affected Platforms

- Cisco Nexus 9000 Series Application Centric Infrastructure.

Summary

As the leading trusted secure cyber coordination center in the region, aeCERT has researched and discovered a vulnerability in the SSH key management of Cisco Nexus 9000 Application Centric Infrastructure (ACI) Mode Switch Software. The exploit of this vulnerability could allow an unauthenticated attacker to gain remote access with root user privileges. This vulnerability is present due to the default SSH key pair present in the 9000 series. All Cisco Nexus 9000 Series Devices with Software Release prior to 14.1(1i) are vulnerable. Cisco has addressed this vulnerability by releasing a software update for the affected devices running software prior to 14.1(1i).

Threat Details

Cisco Nexus 9000 Series ACI Mode Switch leverages SSH protocol that can be used to establish remote connections. All of Cisco Nexus 9000 Series ACI Mode Switch Software prior to 14.1(1i) are affected due to a default SSH key pair that is present in these devices. Threat actors could exploit this vulnerability by opening an SSH connection via IPv6 to a targeted device using the extracted default key materials. The exploit of this vulnerability could allow an unauthenticated attacker to gain remote access with root user privileges. This vulnerability is only exploitable over IPv6; IPv4 is not vulnerable to this attack.

To identify whether the device is vulnerable, administrators can use the show version command in the CLI:

```
switch# show version
Cisco Nexus Operating System (NX-OS) Software
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
Software
BIOS:      version N/A
kickstart: version 11.2(2)  [build 11.2(1.184)]
system:    version 11.2(2)  [build 11.2(1.184)]
```

Solution

In order to circumvent the exploit, we highly recommend the following:

Cisco has released software updates that address the mentioned vulnerabilities. We recommend updating your software as soon as possible.

The vulnerability is fixed in versions 14.1(1i) and above.

References

Cisco

Contact Us

aeCERT
P.O. Box 116688
Dubai, United Arab Emirates

Tel (+971) 4 777 4003
Fax (+971) 4 777 4100
Email info[at]aeCERT.ae
Instagram @TheUAETRA
Twitter @TheUAETRA

For secure communications with aeCERT with regards to sensitive or vulnerability information please send your correspondences to aeCERT[at]aeCERT.ae