Security Advisory 2019-011

Cisco Critical Vulnerability Affecting Nexus 9000 Switches

May 3, 2019 — v1.0

TLP:WHITE

History:

- *3/05/2019 — v1.0 – Initial publication*

Summary

A critical vulnerability affecting Nexus 9000 switches has been recently disclosed. The vulnerability identified as CVE-2019-1804 is a hardcoded SSH key pair that could allow an unauthenticated, remote attacker to connect to the affected system with the privileges of the root user.

Technical Details

The vulnerability is due to the presence of a default SSH key pair that is present in all affected devices. An attacker could exploit this vulnerability by opening an SSH connection via IPv6 to a targeted device using the extracted key materials. An exploit could allow the attacker to access the system with the privileges of the *root* user. This vulnerability is only exploitable over IPv6 – IPv4 is not vulnerable [1].

Products Affected

This vulnerability affects Cisco Nexus 9000 Series Application Centric Infrastructure (ACI) Mode Switch Software.

Recommendations

There are no workarounds to address this vulnerability. Cisco has released software updates to fix the defective software and for other issues [2].

References

[1] https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190501-nexus9k-sshkey

[2] https://tools.cisco.com/security/center/publicationListing.x