



# Advisory Alert

Alert Number : AAA20200828

Date : August 28, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

## Overview

Product	Severity	Vulnerability
Cisco	High	Multiple Vulnerabilities

## Description

Affected Product	Cisco
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3504) (CVE-2019-1896) (CVE-2020-3338) (CVE-2018-0306) (CVE-2018-0307) (CVE-2020-3454) (CVE-2020-3397) (CVE-2020-3398) (CVE-2020-3394) (CVE-2020-3415) (CVE-2020-3517) (CVE-2020-3452)
Description	Cisco has released patch updates addressing multiple vulnerabilities that exists in Cisco switches, Routers and Security Appliance. These vulnerabilities is include Privilege Escalation, Denial of Service, Arbitrary Command, Path Traversal, Injection Remote Code Execution could support an unauthenticated attacker with gain unauthorized access to vulnerable devices.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	<a href="https://tools.cisco.com/security/center/publicationListing.x">https://tools.cisco.com/security/center/publicationListing.x</a>

## Disclaimer

The information provided herein is on "as is" basis, without warranty of any kind. FinCSIRT highly recommend to follow the company policies and procedures when applying the necessary patches with thorough testing and ensuring proper roll-back capabilities exists.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaClear Pvt Ltd, Level 18, Bank of Ceylon Head Office, BOC Square, 01 Bank of Ceylon Mawatha, Colombo 00100, Sri Lanka

Hotline: + 94 112039777

Report incident to [incident@fincsirt.lk](mailto:incident@fincsirt.lk)