Advisory Alert

Alert Number: AAA20211207 **Date:** December 7, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-34779, CVE-2021-34780, CVE-2021-34775, CVE-2021-34776, CVE-2021-34777, CVE-2021-34778)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. In order to exploit these vulnerabilities, the attacker must be in the same broadcast domain as the affected device and successful exploitation of the vulnerabilities could lead an unauthenticated attacker to execute code on the affected device/ cause it to reload unexpectedly or cause LLDP database corruption on the affected device. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Small Business 220 Series Smart Switches
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb220-lldp-multivuls-mVRUtQ8T#vp

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.