Advisory Alert

Alert Number: AAA20220928 **Date:** September 28, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Medium**	Security Restriction Bypass vulnerability

Description

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Security Restriction Bypass vulnerability (CVE-2022-20728)
Description	Cisco has released Security Updates addressing a security restriction bypass vulnerability that exist in their products. An attacker could exploit this vulnerability by gaining access to the native VLAN and forwarding traffic directly to the client via their MAC/IP combination. A successful exploit would allow the attacker to bypass VLAN allocation and bypass any Layer 3 security mechanisms that are deployed. Cisco recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	All versions of 6300 Series Embedded Services Access Points All versions of Cisco Aironet 1540 Series Access Points All versions of Cisco Aironet 1560 Series Access Points All versions of Cisco Aironet 1800 Access Points All versions of Cisco Aironet 2800 Series Access Points All versions of Cisco Aironet 3800 Series Access Points All versions of Cisco Aironet 4800 Access Points All versions of Business 100 Series Access Points All versions of Business 200 Series Access Points All versions of Cisco Catalyst 9100 All versions of Catalyst IW6300 AC Heavy Duty Access Point All versions of Integrated AP on 1100 Integrated Services Routers Cisco Wireless LAN Controller: before 8.10MR8 Cisco Catalyst 9800 Wireless Controller: before 17.6.2, 17.3.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-apvlan-TDTtb4FY

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.