Advisory Alert

Alert Number: AAA20210603 **Date:** June 3, 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-2021-1528, CVE-2021-1539, CVE-2021-1540)
Description	CVE-2021-1528 – Privilege Escalation vulnerability in the CLI of Cisco SD-WAN Software could allow an authenticated, local attacker to gain elevated privileges on an affected system. CVE-2021-1539, CVE-2021-1540 – Authorization Bypass Vulnerability in the authorization process of Cisco ASR 5000 Series Software could allow an authenticated, remote attacker to bypass authorization and execute a subset of CLI commands on an affected device.
Affected Products	SD-WAN vBond Orchestrator Software SD-WAN vEdge Cloud Routers SD-WAN vEdge Routers SD-WAN vManage Software SD-WAN vSmart Controller Software ASR 5000 Series Aggregation Services Routers Virtualized Packet Core – Distributed Instance (VPC-DI) Virtualized Packet Core – Single Instance (VPC-SI)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-fuErCWwF https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asr5k-autho-bypass-mJDF5S7n

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.