Advisory Alert

Alert Number: AAA20210203 **Date:** February 03, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical** **High** **High**	Command Injection Vulnerabilities Denial of Service Vulnerabilities Authorization Bypass Vulnerabilities

Description

Affected Product	**Cisco SD-WAN**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerabilities(CVE-2021-1260, CVE-2021-1261, CVE-2021-1262, CVE-2021-1263, CVE-2021-1298, CVE-2021-1299)
Description	Cisco SD-WAN products are affected with multiple vulnerabilities that could permit a validated attacker to perform command injection attacks against an influenced device, A successful exploitation of the vulnerability would allow an attacker to execute arbitrary code on the underlying operating system with root privileges.
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
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-cmdinjm-9QMSmgcn

Affected Product	**Cisco SD-WAN**
Severity	**High**
Affected Vulnerability	Denial of Service (CVE-2021-1241, CVE-2021-1273, CVE-2021-1274, CVE-2021-1278, CVE-2021-1279)
Description	A buffer overflow condition in Cisco's SD-WAN products lets authenticated remote attackers send specially crafted files to vulnerable devices, resulting in a denial of service condition.
Affected Products	IOS XE SD-WAN Software SD-WAN vBond Orchestrator Software SD-WAN vEdge Cloud Routers SD-WAN vEdge Routers SD-WAN vManage Software SD-WAN vSmart Controller Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-dosmulti-48jJuEUP

Affected Product	**Cisco SD-WAN vManage**
Severity	**High**
Affected Vulnerability	Authorization Bypass Vulnerabilities(CVE-2021-1302, CVE-2021-1304, CVE-2021-1305)
Description	An authorization bypass vulnerability exists in the web-based management interface due to insufficient authorization checks. A successful exploit could allow authenticated, remote attackers to perform activities on an affected system that they are not authorized to perform.
Affected Products	IOS XE SD-WAN Software SD-WAN vBond Orchestrator Software SD-WAN vEdge Cloud Routers SD-WAN vEdge Routers SD-WAN vSmart Controller Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-abyp-TnGFHrS

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.