Advisory Alert

Alert Number: AAA20210510 **Date:** May 10, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	**Multiple Vulnerabilities**
Cisco	**Critical**	**Command Injection Vulnerabilities**
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1275, CVE-2021-1468, CVE-2021-1505, CVE-2021-1508, CVE-2021-1506**)**
Description	Cisco SD-WAN vManage Software is found to be affected to Multiple vulnerabilities that could allow an unauthenticated, remote attacker to execute arbitrary code or gain access to sensitive information. An authenticated, local attacker could gain unauthorized access to the application through privilege escalation upon a successful exploit of these vulnerabilities.
Affected Products	Cisco SD-WAN vManage Software version 18.4 and earlier, 19.2, 20.1, 20.3, 20.4, 20.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sd-wan-vmanage-4TbynnhZ#fs

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Command Injection Vulnerabilities (CVE-2021-1497, CVE-2021-1498)
Description	Web-based management interface of Cisco HyperFlex HX Data Platform is found to be affected by a vulnerability that could allow an unauthenticated, remote attacker to perform a command injection attack against an affected device due to insufficient validation of user-supplied input. This vulnerability could ultimately lead an attacker to execute arbitrary commands on an affected device as the **root** or **tomcat8** user upon a successful exploit.
Affected Products	HyperFlex HX: 4.0, 4.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1426, CVE-2021-1427, CVE-2021-1428, CVE-2021-1429, CVE-2021-1430, CVE-2021-1496)
Description	Cisco AnyConnect Secure Mobility Client for Windows is found to be affected with Multiple vulnerabilities in the install, uninstall, and upgrade processes that could allow an authenticated, local attacker to hijack DLL or executable files that are used by the application. These vulnerabilities could lead an attacker to execute arbitrary code on an affected device with *SYSTEM* privileges upon a successful exploit.
Affected Products	Cisco AnyConnect Secure Mobility Client for Windows version Earlier than 4.9.06037, 4.10.00093 and 4.9.03022
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-code-exec-jR3tWTA6

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.