Advisory Alert

Alert Number: AAA20220505 **Date:** May 5, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Root Level Command Execution Vulnerability
HP	**High**	Multiple Vulnerabilities
Cisco	**Medium**	Multiple Vulnerabilities

Description

Affected Product	Cisco
Severity	**Critical**
Affected Vulnerability	Root Level Command Execution Vulnerability
Description	Cisco Enterprise NFV Infrastructure Software (NFVIS) has multiple vulnerabilities which might allow an attacker to gain access to the host computer via the guest virtual machine (VM), insert root-level commands, or leak system data from the host to the VM. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Cisco Enterprise NFVIS Earlier than 4.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-NFVIS-MUL-7DySRX9

Affected Product	HP
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2021-21419, CVE-2021-33503, CVE-2022-23657,CVE-2022-23658, CVE-2022-23659, CVE-2022-23660, CVE-2022-23661, CVE-2022-23662, CVE-2022-23663, CVE-2022-23664, CVE-2022-23665, CVE-2022-23666, CVE-2022-23667, CVE-2022-23668, CVE-2022-23669, CVE-2022-23670, CVE-2022-23671, CVE-2022-23672, CVE-2022-23673, CVE-2022-23674, CVE-2022-23675, CVE-2022-23676, CVE-2022-23677)
Description	HP has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the vulnerabilities could cause Arbitrary Command Execution, Authentication Bypass, Cross-Site Scripting (XSS), Disclosure of Sensitive Information, and Server-Side Request Forgery (SSRF). Cisco highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	ClearPass Policy Manager 6.10.x: 6.10.4 and below ClearPass Policy Manager 6.9.x: 6.9.9 and below ClearPass Policy Manager 6.8.x: 6.8.9-HF2 and below ArubaOS-Switch 15. All versions. ArubaOS-Switch 16. All versions. ArubaOS-Switch 16.08.xxxx: KB/WB/WC/YA/YB/YC.16.08.0024 and below. ArubaOS-Switch 16.09.xxxx: KB/WB/WC/YA/YB/YC.16.09.0019 and below. ArubaOS-Switch 16.10.xxxx: KB/WB/WC/YA/YB/YC.16.10.0019 and below. ArubaOS-Switch 16.11.xxxx: KB/WB/WC/YA/YB/YC.16.11.0003 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04279en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04285en_us https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04291en_us

Affected Product	Cisco
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-20796, CVE-2022-20785, CVE-2022-20770, CVE-2022-20771, CVE-2022-20734, CVE-2022-20799, CVE-2022-20801, CVE-2022-20753, CVE-2022-20764, CVE-2022-20794)
Description	Cisco has released security updates addressing multiple vulnerabilities that exists in their products. Successful exploitation of the most severe vulnerabilities could cause Denial of Service, Memory Leak vulnerability, Disclosure of Sensitive Information and Remote code execution. Cisco highly recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Secure Endpoint, formerly Advanced Malware Protection (AMP) for Endpoints, for Linux Secure Endpoint, formerly AMP for Endpoints, for MacOS Secure Endpoint, formerly AMP for Endpoints, for Windows Cisco SD-WAN vManage Software 20.5 and earlier Cisco SD-WAN vManage Software 20.6, 20.7, 20.8 Cisco Small Business Router Firmware 1.0.03.26 and earlier Cisco TelePresence CE Software Earlier than 9 Cisco TelePresence CE Software 9, 10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-vL9x58p4 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-html-XAuOK8mR https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-prVGcHLd https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-clamav-dos-ZAZBwRVG https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-vmge-infodc-WPSkAMhp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-smb-rv-cmd-inj-8Pv9JMJD https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sbrv-rce-OYLQbL9u https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ROS-DOS-X7H7XhkK

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.