Advisory Alert

Alert Number: AAA20221216 **Date:** December 16, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**Critical**	Multiple Vulnerabilities
RedHat	**High**	Multiple Vulnerabilities
Samba	**High**, **Medium**	Multiple Vulnerabilities
Cisco	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Cisco**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-0147, CVE-2021-1497, CVE-2021-1498, CVE-2018-0125, CVE-2018-0171)
Description	Cisco has released an update for a set of security updates that were released earlier, addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to arbitrary command execution and denial of service. Cisco highly recommends to apply the patch updates at the earliest to avoid issues.
Affected Products	All releases of Cisco Secure ACS prior to release 5.8 patch 9. Cisco devices that are running Cisco HyperFlex HX Software version 4.0, 4.5 and earlier than 4.0 All firmware releases of Cisco RV132W ADSL2+ Wireless-N VPN Router and RV134W VDSL2 Wireless-AC VPN Router Cisco devices that are running a vulnerable release of Cisco IOS or IOS XE Software and have the Smart Install client feature enabled.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180307-acs2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-hyperflex-rce-TjjNrkpR https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180207-rv13x https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-1158, CVE-2022-2639, CVE-2022-2959, CVE-2022-43945)
Description	RedHat has released a security update to address multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to kernel corruption, denial of service and privilege escalation. RedHat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.0 x86_64 Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.0 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.0 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.0 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:9082

Affected Product	**Samba**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-38023, CVE-2022-37966, CVE-2022-37967, CVE-2022-45141, CVE-2022-42898)
Description	Samba has released security updates to address multiple vulnerabilities that exist in their products. If exploited these vulnerabilities could lead to privilege elevation and heap corruption. Samba recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	All versions of Samba
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.samba.org/samba/security/CVE-2022-38023.html https://www.samba.org/samba/security/CVE-2022-37966.html https://www.samba.org/samba/security/CVE-2022-37967.html https://www.samba.org/samba/security/CVE-2022-45141.html https://www.samba.org/samba/security/CVE-2022-42898.html

Affected Product	**Cisco**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2018-0174, CVE-2018-0159, CVE-2018-0172, CVE-2018-0161, CVE-2019-15271, CVE-2018-0158, CVE-2018-0167, CVE-2018-0175, CVE-2018-0173, CVE-2018-0156, CVE-2018-0155, CVE-2018-0179, CVE-2018-0180)
Description	Cisco has released an update for a set of security updates that were released earlier, addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could leads to denial of service, arbitrary code execution with elevated privileges. Cisco recommends to apply the patch updates at the earliest to avoid issues.
Affected Products	Multiple Products and versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-dhcpr3 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-ike-dos https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-dhcpr1 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-snmp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20191106-sbrv-cmd-x https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-ike https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-lldp https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-dhcpr2 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-bfd https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-slogin

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.