Advisory Alert

Alert Number: AAA20210520 **Date:** May 20, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities
RedHat	**Medium**	Sudo security and bug fix update

Description

Affected Product	**Cisco**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-1487, CVE-2021-1531, CVE-2019-1726 CVE-2021-1547, CVE-2021-1548, CVE-2021-1549, CVE-2021-1550, CVE-2021-1551, CVE-2021-1552, CVE-2021-1553, CVE-2021-1554, CVE-2021-1555, CVE-2021-1254, CVE-2021-1358, CVE-2021-1557, CVE-2021-1558, CVE-2021-1559, CVE-2021-1560, CVE-2021-1306)
Description	Cisco has released Security Updates addressing multiple vulnerabilities that exists with multiple Cisco products. Most of them severe could allow a remote attacker to take control of an affected system. It is highly recommended by Cisco to apply necessary security fixes at earliest to avoid issues.
Affected Products	Multiple products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-pi-epnm-cmd-inj-YU5e6tB3 https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cml-cmd-inject-N4VYeQXB https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20190515-nxos-cli-bypass https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sb-wap-inject-Mp9FSdG https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-strd-xss-bUKqffFW https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-finesse-opn-rdrct-epDeh7R https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnasp-conn-prvesc-q6T6BzW https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-dnasp-conn-cmdinj-HOj4YV5n https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ade-xcvAQEOZ

Affected Product	**RedHat**
Severity	**Medium**
Affected Vulnerability	Sudo security and bug fix update(CVE-2021-23239, CVE-2021-23240)
Description	CVE-2021-23239 -The sudoedit personality of Sudo before 1.9.5 may allow a local unprivileged user to perform arbitrary directory-existence tests by winning a sudo_edit.c race condition in replacing a user-controlled directory by a symlink to an arbitrary path. Data confidentiality is threatened from this vulnerability. CVE-2021-23240 - selinux_edit_copy_tfiles in sudoedit in Sudo before 1.9.5 allows a local unprivileged user to gain file ownership and escalate privileges by replacing a temporary file with a symlink to an arbitrary file target. This affects SELinux RBAC support in permissive mode.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2021:1723 https://access.redhat.com/security/cve/CVE-2021 23239?extIdCarryOver=true&sc_cid=701f2000001OH7JAAW https://access.redhat.com/security/cve/CVE-2021- 23240?extIdCarryOver=true&sc_cid=701f2000001OH7JAAW

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.