TLP: WHITE

Advisory Alert

Alert Number : **AAA20200903** **Date :** **September 3, 2020**

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Cisco	**High**	Multiple Vulnerabilities
Red Hat	**High**	Security and bug fix update

Description

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities(CVE-2020-3495, CVE-2020-3478, CVE-2020-3430, CVE-2020-3530, CVE-2020-3473, CVE-2020-3542, CVE-2020-3541, CVE-2020-3547, CVE-2020-3451, CVE-2020-3453, CVE-2020-3365, CVE-2020-3537, CVE-2020-3545,CVE-2020-3548, CVE-2020-3546, CVE-2020-3440)
Description	Cisco has released patch updates addressing multiple vulnerabilities including These vulnerabilities include Information Disclosure, Denial of Service, buffer overflow, Path Traversal, command Injection and Remote Code Execution across several of its products. Some of this vulnerabilities could allow an unauthenticated attacker with gain unauthorized access to vulnerable devices.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/publicationListing.x

Affected Product	Red Hat
Severity	**High**
Affected Vulnerability	ansible: dnf module install packages with no GPG signature(CVE-2020-14365)
Description	Redhat has released a Security Update to address a newly found flaw in Ansible, which may lead to malicious packages being installed on the system and arbitrary code executed via package installation scripts. This vulnerability directly poses a serious threat to integrity and system availability.
Affected Products	Red Hat Ansible Engine 2.8 for RHEL 8 x86_64 Red Hat Ansible Engine 2.8 for RHEL 8 s390x Red Hat Ansible Engine 2.8 for RHEL 8 ppc64le Red Hat Ansible Engine 2.8 for RHEL 8 aarch64 Red Hat Ansible Engine 2.8 for RHEL 7 x86_64 Red Hat Ansible Engine 2.8 for RHEL 7 s390x Red Hat Ansible Engine 2.8 for RHEL 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2020:3600 https://access.redhat.com/security/cve/CVE-2020-14365

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.