Advisory Alert

Alert Number : AAA20200729 **Date :** July 29, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Red Hat	**Critical**	Denial of Service
Citrix	**High**	Privilege Escalating
CISCO	**High**	Path Traversal Vulnerability

Description

Affected Product	Red Hat
Severity	**Critical**
Affected Vulnerability	Denial of Service (CVE-2020-10740) (CVE-2020-14307) (CVE-2020-14297)
Description	This security update fixes multiple flows in Red Hat JBoss Enterprise Application Platform which based on the WildFly runtime causing Denial of Service. Additionally the services that are addressed in this update can be listed as Wildfly Enterprise Java Beans, jboss-ejb-client and jboss-ejb-client wildfly related services.
Affected Products	Red Hat JBoss Enterprise Application Platform 7.3.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2020:3143 https://access.redhat.com/security/cve/CVE-2020-10740?extIdCarryOver=true&sc_cid=701f2000001OH6kAAG https://access.redhat.com/security/cve/CVE-2020-14297?extIdCarryOver=true&sc_cid=701f2000001OH6kAAG https://access.redhat.com/security/cve/CVE-2020-14307?extIdCarryOver=true&sc_cid=701f2000001OH6kAAG

Affected Product	Citrix
Severity	**High**
Affected Vulnerability	Privilege Escalating (CVE-2020-8207)
Description	This vulnerability will cause an automatic update on a computer running workspace app by escalating local user privilege level to an administrators privileges. As a result of this flow, a computer running Citrix Workspace app when Windows file sharing (SMB) is enabled can be compromised remotely.
Affected Products	Citrix Workspace app for Windows 1912 LTSR Citrix Workspace app for Windows 2002
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX277662

Affected Product	CISCO
Severity	**High**
Affected Vulnerability	Path Traversal Vulnerability (CVE-2020-3452)
Description	CISCO ASA Firewall and CISCO FTD (Threat Defense) systems could allow an unauthenticated, remote attacker to conduct directory path traversal attacks and read sensitive files on a targeted system.
Affected Products	Cisco ASA Software Cisco FTD Software
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-asaftd-ro-path-KJuQhB86

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.