Advisory Alert

Alert Number : AAA20200819 **Date :** August 19, 2020

Document Classification Level : Public Circulation Permitted

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**High**	Multiple Vulnerabilities
RedHat	**High**	Multiple Vulnerabilities
Apache	**High**	Multiple Vulnerabilities
HP	**High**	Multiple Vulnerabilities
Cisco	**High**	Multiple Vulnerabilities

Description

Affected Product	IBM
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-2590, CVE-2020-2601)
Description	IBM has released patch updates addressing multiple vulnerabilities that exists in IBM WebSphere Application that comes with IBM security access manager for enterprise single sign-on that uses Java SE, Java SE Embedded security component. These vulnerabilities could lead an unauthenticated attacker with network access via Kerberos to gain unauthorized access to critical data and cause no confidentiality, integrity, availability impact.
Affected Products	IBM Security Access Manager for Enterprise Single-Sign On 8.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6260521

Affected Product	RedHat
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-10718, CVE-2020-10683, CVE-2020-10714, CVE-2020-10687, CVE-2020-10673, CVE-2019-14900, CVE-2020-10740, CVE-2020-10672, CVE-2020-1710, CVE-2020-10693, CVE-2020-1748, CVE-2020-14297)
Description	RedHat has released security updates addressing multiple component vulnerabilities in Red Hat JBoss Enterprise Application Platform 7 which is used as a platform for Java applications based on WildFly application runtime. This contains bug fixes for wildfly, dom4j, wildfly-elytron, wildfly-undertow, jackson-databind, hibernate-core, undertow, hibernate-validator.
Affected Products	Red Hat JBoss Enterprise Application Platform 7.3.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2020:3464

Affected Product	Apache
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-9490, CVE-2020-11984, CVE-2020-11993)
Description	Apache software foundation has released security patches addressing multiple vulnerabilities. Successful exploitation could allow an attacker to execute remote code execution in the context of affected application. Based on the privileges associated with the application the attacker can view, edit, or delete data.
Affected Products	Apache versions 2.4.43 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://httpd.apache.org/security/vulnerabilities_24.html

Affected Product	HP
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-11896, CVE-2020-11898, CVE-2020-11900, CVE-2020-11906, CVE-2020-11907, CVE-2020-11911, CVE-2020-11912, CVE-2020-11914)
Description	HP iLO is a remote server management processor embedded on system boards of HP servers which allows controlling and monitoring HP servers from a remote location and HPE has released updates addressing multiple vulnerabilities that exists in HP iLO. The vulnerabilities could be remotely exploited to execute code, cause denial of service, and expose sensitive information. It is highly recommended to apply necessary updates as soon as possible.
Affected Products	HPE Integrated Lights-Out 3 (iLO 3) -Prior to v1.93 HPE Integrated Lights-Out 4 (iLO 4) -Prior to v2.75 HPE Integrated Lights-Out 5 (iLO 5) for HPE Gen10 Servers -Prior to v2.18
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04012en_us

Affected Product	Cisco
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-3435, CVE-2020-3433, CVE-2020-3434)
Description	Cisco AnyConnect is a unified endpoint agent which is capable in delivering multiple security services to protect the enterprise. Cisco has released security patches addressing multiple vulnerabilities that exists in Cisco AnyConnect Secure Mobiliti Client for Windows. An attacker could use these vulnerabilities and perform overwriting VPN profiles, DLL hijacking attack and cause denial of service attacks on affected devices.
Affected Products	Cisco AnyConnect Secure Mobility Client for Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-profile-7u3PERKF https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dll-F26WwJW https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-dos-feXq4tAV

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.