Advisory Alert

Alert Number: AAA20210630 **Date:** June 30, 2021

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	High	Multiple Vulnerabilities
Redhat	Medium	Signature checks bypass via corrupted rpm package

Description

Affected Product	IBM
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-20572, CVE-2021-20494, CVE-2021-20574, CVE-2021-20488, CVE-2021-20573, CVE-2021-3449 , CVE-2021-3450, CVE-2021-23839, CVE-2021-23840, CVE-2021-26691, CVE-2021-26690)
Description	IBM has released security updates addressing multiple vulnerabilities that exists in their products. The most severe vulnerability could cause denial of service and account take over and IBM highly recommends to apply necessary security fixes to avoid issues.
Affected Products	IBM Security Identity Manager Adapters 6.0, 7.0 IBM Integration Bus V10.0.0 - V10.0.0.23 IBM App connect Enterprise V11 , V11.0.0.0 - V11.0.0.12 IBM App connect Enterprise V12.0.1.0 IBM App connect Enterprise V12 IBM HTTP Server 9.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/6467651 https://www.ibm.com/support/pages/node/6463979 https://www.ibm.com/support/pages/node/6466315 https://www.ibm.com/support/pages/node/6465875

Affected Product	Redhat
Severity	Medium
Affected Vulnerability	Signature checks bypass via corrupted rpm package (CVE-2021-20271)
Description	Redhat has released security updates addressing signature check bypass vulnerability that exists in their products. Using this flaw a malicious actor can convince a victim to install a seemingly verifiable package, whose signature header was modified, to cause RPM database corruption and execute code. Redhat highly recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 8.4 x86_64 Red Hat Enterprise Linux Server - AUS 8.4 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 8.4 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 8.4 ppc64le Red Hat Enterprise Linux Server - TUS 8.4 x86_64 Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 8.4 aarch64 Red Hat Enterprise Linux Server (for IBM Power LE) - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux Server - Update Services for SAP Solutions 8.4 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/security/cve/CVE-2021-20271

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.