Advisory Alert

Alert Number: AAA20230605 **Date:** June 5, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**	Remote Code Execution Vulnerability
IBM	**High**	Information Disclosure Vulnerability
HPE	**Medium**	Arbitrary Code Execution Vulnerability

Description

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2023-24805)
Description	Red Hat has released a security update for the Remote Code Execution Vulnerability to address that could potentially be exploited by attackers. Cups-filters provides backends, filters, and other software for the Common UNIX Printing System (CUPS) project. RedHat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for x86_64 9 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux for IBM z Systems 9 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for Power, little endian 9 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for ARM 64 9 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 9 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 9 ppc64le Red Hat CodeReady Linux Builder for ARM 64 9 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 9 s390x Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux Server for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux Server for IBM z Systems - 4 years of updates 9.2 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2023:3423

Affected Product	**IBM**
Severity	**High**
Affected Vulnerability	Information Disclosure Vulnerability **(**CVE-2023-32342**)**
Description	IBM has released a security update for IBM WebSphere Remote Server. This vulnerability could allow a remote attacker to obtain sensitive information. A remote attacker can send an overly large number of trial messages for decryption and perform a timing-based side channel attack against the RSA Decryption implementation. IBM recommends to apply the necessary patch updates at your earliest to avoid issues
Affected Products	IBM WebSphere Remote Server 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7000993

Affected Product	**HPE**
Severity	**Medium**
Affected Vulnerability	Arbitrary Code Execution Vulnerability (CVE-2020-7205)
Description	HPE has released a security update addressing Arbitrary Code Execution Vulnerability in HPE Smart Storage Administrator (SSA) Offline. This vulnerability could be locally exploited to allow arbitrary code execution during the boot process when using insmod in GRUB2 in the specific impacted HPE product. HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE Smart Storage Administrator (SSA) -All Offline versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbhf04484en_us

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.