Advisory Alert

Alert Number: AAA20221005 **Date:** October 5, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Redhat	**High**	Multiple Vulnerabilities

Description

Affected Product	**Redhat**
Severity	**High**
Affected Vulnerability	Multiple vulnerabilities (CVE-2022-41318, CVE-2022-38177, CVE-2022-38178)
Description	RedHat has released Security Updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-41318** - An incorrect integer overflow protection in the Squid SSPI and SMB authentication helpers is vulnerable to a buffer overflow attack, resulting in information disclosure or a denial of service in Squid **CVE-2022-38177** - Bind package flow was spoofing the target resolver with responses that have a malformed ECDSA signature, an attacker can trigger a small memory leak. It is possible to gradually erode available memory to the point where named crashes for lack of resources. **CVE-2022-38178** - Bind package flaw was spoofing the target resolver with responses that have a malformed EdDSA signature, an attacker can trigger a small memory leak. RedHat recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.1 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.1 x86_64 Red Hat Enterprise Linux Server 7 x86_64 Red Hat Enterprise Linux Workstation 7 x86_64 Red Hat Enterprise Linux Desktop 7 x86_64 Red Hat Enterprise Linux for IBM z Systems 7 s390x Red Hat Enterprise Linux for Power, big endian 7 ppc64 Red Hat Enterprise Linux for Scientific Computing 7 x86_64 Red Hat Enterprise Linux for Power, little endian 7 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:6774 https://access.redhat.com/errata/RHSA-2022:6765

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.