Advisory Alert

Alert Number: AAA20221130 **Date:** November 30, 2022

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
RedHat	**High**	Denial Of Service Vulnerability
SUSE	**High**	Multiple Vulnerabilities
VMware	**Low**	Denial Of Service Vulnerability

Description

Affected Product	**RedHat**
Severity	**High**
Affected Vulnerability	Denial Of Service Vulnerability (CVE-2022-1158)
Description	RedHat has released security updates addressing a denial of service vulnerability that exist in their products. **CVE-2022-1158** – A denial of service vulnerability that exsist because of a flaw found in KVM. When updating a guest's page table entry, vm_pgoff was improperly used as the offset to get the page's pfn. As vaddr and vm_pgoff are controllable by user-mode processes, this flaw allows unprivileged local users on the host to write outside the userspace region and potentially corrupt the kernel, resulting in a denial of service condition. RedHat highly recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat Enterprise Linux for Real Time - Telecommunications Update Service 8.4 x86_64 Red Hat Enterprise Linux for Real Time for NFV - Telecommunications Update Service 8.4 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 - Extended Update Support 8.4 s390x 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 - Extended Update Support 8.4 aarch64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.4 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.4 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 8.4 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 8.4 ppc64le Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 8.4 aarch64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2022:8685 https://access.redhat.com/errata/RHSA-2022:8673

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-4037, CVE-2022-2153, CVE-2022-2964, CVE-2022-3169, CVE-2022-3424, CVE-2022-3521, CVE-2022-3524, CVE-2022-3542, CVE-2022-3545, CVE-2022-3565, CVE-2022-3586, CVE-2022-3594, CVE-2022-3621, CVE-2022-3629, CVE-2022-3646, CVE-2022-3649, CVE-2022-40307, CVE-2022-40768, CVE-2022-42703, CVE-2022-43750)
Description	SUSE has released a security update addressing multiple vulnerabilities that affect the Linux kernel. Successful exploitation of the most severe vulnerabilities could cause denial of service, memory corruption and leakage, and create a race condition. SUSE recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	SUSE Linux Enterprise Desktop 12-SP5 SUSE Linux Enterprise High Availability 12-SP5 SUSE Linux Enterprise High Performance Computing 12-SP5 SUSE Linux Enterprise Live Patching 12-SP5 SUSE Linux Enterprise Server 12-SP5 SUSE Linux Enterprise Server for SAP Applications 12-SP5 SUSE Linux Enterprise Software Development Kit 12-SP5 SUSE Linux Enterprise Workstation Extension 12-SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2022/suse-su-20224272-1/

Affected Product	**VMware**
Severity	**Low**
Affected Vulnerability	Denial of Service Vulnerability (CVE-2022-31693)
Description	VMware has released a security update to address a denial of service vulnerability that exists in the VMware Tools for Windows. **CVE-2022-31693** - VMware Tools for Windows contains a denial-of-service vulnerability in the VM3DMP driver. Using this vulnerability, a malicious actor with local user privileges in the Windows guest OS, where VMware Tools is installed, can trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest OS. VMware recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	VMware Tools for Windows 12.x.y, 11.x.y and 10.x.y
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2022-0029.html

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.