Advisory Alert

Alert Number: AAA20230807 **Date:** August 7, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
VMware	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20593, CVE-2023-2985, CVE-2023-3117, CVE-2023-31248, CVE-2023-3390, CVE-2023-35001, CVE-2023-3609, CVE-2023-3611, CVE-2023-3812)
Description	Suse has released security updates addressing multiple vulnerabilities affecting their products. Exploitation of these vulnerabilities could lead to Use-after-free condition, out-of-bounds write, out-of-bounds memory access, denial of service. Suse recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	openSUSE Leap 15.4 openSUSE Leap 15.5 Public Cloud Module 15-SP4 Public Cloud Module 15-SP5 SUSE Linux Enterprise High Performance Computing 15 SP4 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Server 15 SP4 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Manager Proxy 4.3 SUSE Manager Retail Branch Server 4.3 SUSE Manager Server 4.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20233182-1/ https://www.suse.com/support/update/announcement/2023/suse-su-20233180-1/

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34037, CVE-2023-34038)
Description	VMware has released a security update addressing multiple vulnerabilities affecting VMware Horizon Server. If exploited these vulnerabilities could lead to Request smuggling and Information disclosure. **CVE-2023-34037-** By exploiting this vulnerability, A malicious actor with network access may be able to perform HTTP smuggle requests. **CVE-2023-34038-** By exploiting this vulnerability, A malicious actor with network access may be able to access information relating to the internal network configuration VMware recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	VMware Horizon Server 2303 VMware Horizon Server 2212 VMware Horizon Server 2209, 2206 VMware Horizon Server 2111.x, 2106, 2103, 2012, 2006
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0017.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.