Advisory Alert

Alert Number: AAA20240306 **Date:** March 6, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
VMware	**Critical**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
SUSE	**High**	Security updates

Description

Affected Product	**VMware**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22252, CVE-2024-22253, CVE-2024-22254, CVE-2024-22255)
Description	VMware has released security updates addressing multiple vulnerabilities that exist in VMware ESXi, Workstation and Fusion. Exploitation of these vulnerabilities may result in Code execution, Out of bound writes and Information disclosure. VMware recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	ESXi 8.0, 7.0 Workstation 17.x Fusion 13.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2024-0006.html

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE: CVE-2024-1356, CVE-2024-25611, CVE-2024-25612, CVE-2024-25613, CVE-2024-25614, CVE-2024-25615, CVE-2024-25616)
Description	HPE has released a security update addressing multiple vulnerabilities in HPE ArubaOS. Exploitation of these vulnerabilities by an attacker, could lead to Arbitrary File Deletion, Remote Arbitrary Code Execution, Denial of Service (DoS), Disclosure of Sensitive Information HPE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	HPE Aruba Networking • Mobility Conductor (formerly Mobility Master) • Mobility Controllers • WLAN Gateways and SD-WAN Gateways managed by Aruba Central Affected Software Versions: • ArubaOS 10.5.x.x: 10.5.0.1 and below • ArubaOS 10.4.x.x: 10.4.0.3 and below • ArubaOS 8.11.x.x: 8.11.2.0 and below • ArubaOS 8.10.x.x: 8.10.0.9 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docLocale=en_US&docId=hpesbnw04604en_us

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Security update (CVE-2022-42265, CVE-2024-0074, CVE-2024-0075)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in kernel firmware. Vulnerability exploitation could lead to Null pointer difference, Buffer overwrite, Integer overflow. SUSE recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Basesystem Module 15-SP5 openSUSE Leap 15.4, 15.5 Public Cloud Module 15-SP5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5 SUSE Linux Enterprise Desktop 15 SP5. 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise High Performance Computing 15 SP4, 15 SP5 SUSE Linux Enterprise High Performance Computing ESPOS 15 SP4 SUSE Linux Enterprise High Performance Computing LTSS 15 SP4 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4 SUSE Linux Enterprise Server 15 SP4 LTSS 15-SP4 SUSE Linux Enterprise Server for SAP Applications 15 SP4 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/2024/suse-su-20240772-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240770-1/

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.