Advisory Alert

Alert Number: AAA20240207 **Date:** February 7, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Suse	**High**	Multiple Vulnerabilities
VMware	**High**	Multiple Vulnerabilities
Veeam	**High**, **Medium**	Privilege Escalation Vulnerabilities
Cisco	**Medium**	Access Control Policy Bypass Vulnerability
Redhat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Suse**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5178, CVE-2023-6176, CVE-2023-6932, CVE-2023-1829)
Description	Suse has released security updates addressing Multiple Vulnerabilities that exist in their products. If exploited by an attacker it could lead to Local privilege escalation, Denial of service and User after free condition. Suse recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	OpenSUSE Leap 15.4, 15.5 SUSE Linux Enterprise High Performance Computing 12 SP5, 15 SP1, 15 SP2, 15 SP4, 15 SP5 SUSE Linux Enterprise Live Patching 12-SP5, 15-SP1, 15-SP2, 15-SP4, 15-SP5 SUSE Linux Enterprise Micro 5.3, 5.4, 5.5 SUSE Linux Enterprise Real Time 15 SP4, 15 SP5 SUSE Linux Enterprise Server 12 SP5, 15 SP1, 15 SP2, 15 SP4, 15 SP5 SUSE Linux Enterprise Server for SAP Applications 12 SP5,15 SP1,15 SP2,15 SP4, SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240378-1 https://www.suse.com/support/update/announcement/2024/suse-su-20240373-1 https://www.suse.com/support/update/announcement/2024/suse-su-20240377-1 https://www.suse.com/support/update/announcement/2024/suse-su-20240376-1

Affected Product	**VMware**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22237, CVE-2024-22238, CVE-2024-22239, CVE-2024-22240, CVE-2024-22241)
Description	VMware has released security updates addressing Multiple Vulnerabilities that exist in Aria Operations for Networks. If exploited it could lead to Privilege Escalation, Cross Site Scripting and Local File Read. VMware recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	VMware Aria Operations for Networks (formerly vRealize Network Insight) 6.x versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2024-0002.html

Affected Product	**Veeam**
Severity	**High**, **Medium**
Affected Vulnerability	Privilege Escalation Vulnerabilities (CVE-2024-22021, CVE-2024-22022)
Description	Veeam has released security updates addressing Privilege Escalation Vulnerabilities that exist in the Veeam Recovery Orchestrator. The vulnerabilities may allow a low-privileged user to access the NTLM hash of the service account used by the Veeam Orchestrator Server Service. Veeam recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Veeam Availability Orchestrator 4 Veeam Disaster Recovery Orchestrator 5 Veeam Recovery Orchestrator 6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4541

Affected Product	**Cisco**
Severity	**Medium**
Affected Vulnerability	Access Control Policy Bypass Vulnerability (CVE-2023-20246)
Description	Cisco has released security updates addressing Access Control Policy Bypass Vulnerability that exist in their products. If exploited it could allow the attacker to bypass configured access control rules on the affected system. Cisco recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Cisco Firepower Threat Defense (FTD) and Cisco FirePOWER Services if they were running Snort 3. Cisco products running a vulnerable release of Cisco Unified Threat Defense (UTD) Snort Intrusion Prevention System (IPS) Engine for Cisco IOS XE Software or Cisco UTD Engine for Cisco IOS XE SD-WAN Software. • 1000 Series Integrated Services Routers (ISRs) • 4000 Series ISRs • Catalyst 8000V Edge Software • Catalyst 8200 Series Edge Platforms • Catalyst 8300 Series Edge Platforms • Catalyst 8500L Edge Platforms • Cloud Services Routers 1000V • Integrated Services Virtual Router (ISRv)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ftd-snort3acp-bypass-3bdR2BEh

Affected Product	**Redhat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44981, CVE-2023-4759, CVE-2023-44483)
Description	Redhat has released security updates addressing Multiple Vulnerabilities that exist in their products. An attacker could exploit theses to cause Private Key disclosure and Arbitrary file overwrite. Redhat recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Red Hat JBoss Middleware Text-Only Advisories for MIDDLEWARE 1 x86_64 JBoss Enterprise Application Platform 7.4 for RHEL 7 x86_64, RHEL 8 x86_64, RHEL 9 x86_64 JBoss Enterprise Application Platform Text-Only Advisories x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0705 https://access.redhat.com/errata/RHSA-2024:0710 https://access.redhat.com/errata/RHSA-2024:0711 https://access.redhat.com/errata/RHSA-2024:0712 https://access.redhat.com/errata/RHSA-2024:0714

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.