Advisory Alert

Alert Number: **AAA20240117** **Date:** **January 17, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Sonicwall	**Critical**	Stack-based Buffer Overflow vulnerability
Oracle	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Dell	**High**	Incorrect Default Permissions vulnerability
SUSE	**High**	Multiple Vulnerabilities
Citrix	**High, Medium**	Multiple Vulnerabilities

Description

Affected Product	**Sonicwall**
Severity	**Critical**
Affected Vulnerability	Stack-based Buffer Overflow vulnerability (CVE-2023-6340)
Description	Sonicwall has released a security update addressing Stack-based Buffer Overflow vulnerability that exist in Sonicwall Capture Client and NetExtender Windows Client **CVE-2023-6340 -** SonicWall Capture Client version 3.7.10 and NetExtender Client Windows client 10.2.337 and earlier versions are being installed with sfpmonitor.sys driver. The client applications communicate with the driver through queries. The driver method that handles those queries has Stack-based Buffer Overflow vulnerability that allows an attacker to craft a specific query to overwrite kernel memory, causing Denial of Service which potentially leads to code execution in the target operating system. Sonicwall recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Capture Client 3.7.10 and earlier versions. NetExtender Windows Client 10.2.337 (Windows 32 and 64 bit) and earlier versions.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-6340

Affected Product	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released January 2024 Security Updates addressing vulnerabilities in Oracle code and in third-party components included in Oracle products. Oracle strongly recommends to apply necessary security patches at earliest to avoid issues
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpujan2024.html

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3611, CVE-2023-3776, CVE-2023-4128, CVE-2023-4206, CVE-2023-4207, CVE-2023-4208)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to use-after-free, out-of-bounds memory write flaw ,denial of service, privilege escalation It is recommended by Red Hat to apply necessary security fixes at earliest to avoid issues
.Affected Products	Red Hat Enterprise Linux Server - AUS 7.6 x86_64 Red Hat Enterprise Linux Server - AUS 7.7 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2024:0262 https://access.redhat.com/errata/RHSA-2024:0261

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Incorrect Default Permissions Vulnerability (CVE-2024-22428)
Description	Dell has released a security update addressing Incorrect Default Permissions vulnerability that exists in their iDRAC Service Module. **CVE-2024-22428 -** Dell iDRAC Service Module, versions 5.2.0.0 and prior, contain an Incorrect Default Permissions vulnerability. It may allow a local unprivileged user to escalate privileges and execute arbitrary code on the affected system. It is recommended by Dell to apply necessary security fixes at earliest to avoid issues
.Affected Products	iDRAC Service Module version iSM 5.3.0.0 and prior
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000221129/dsa-2024-018-security-update-for-dell-idrac-service-module-for-weak-folder-permission-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2020-26555, CVE-2023-51779, CVE-2023-6121, CVE-2023-6531, CVE-2023-6546, CVE-2023-6606, CVE-2023-6610, CVE-2023-6622, CVE-2023-6931, CVE-2023-6932, CVE-2022-2586)
Description	SUSE has released security updates addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to out of bounds read, heap out-of-bounds write, null pointer dereference, information leak It is recommended by SUSE to apply necessary security fixes at earliest to avoid issues
.Affected Products	OpenSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5, 12 SP5, 15 SP1, 15 SP1 LTSS 15-SP1, 15 SP4, 15 SP1, 15 SP1 LTSS 15-SP1, 15 SP4 SUSE Linux Enterprise Live Patching 15-SP5, 12-SP5, 15-SP1, 15-SP4 SUSE Linux Enterprise Micro 5.5, 5.4, 5.3 SUSE Linux Enterprise Real Time 15 SP5, SP4 SUSE Linux Enterprise Server 15 SP5, SP4, 12 SP5, 15 SP1, 15 SP1 Business Critical Linux 15-SP1, 15 SP1 LTSS 15-SP1 SUSE Linux Enterprise Server for SAP Applications 15 SP5, SP4, 15 SP1, 12 SP5 SUSE Real Time Module 15-SP5, 15-SP4 SUSE Linux Enterprise High Availability Extension 12 SP5, 15 SP1 SUSE Linux Enterprise Software Development Kit 12 SP5 SUSE Linux Enterprise Workstation Extension 12 12-SP5 SUSE CaaS Platform 4.0 SUSE Manager Proxy 4.0 SUSE Manager Retail Branch Server 4.0 SUSE Manager Server 4.0 OpenSUSE Leap Micro 5.3, 5.4 SUSE Linux Enterprise Micro for Rancher 5.3, 5.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20240115-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240117-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240120-1/ https://www.suse.com/support/update/announcement/2024/suse-su-20240129-1/

Affected Product	**Citrix**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-5914, CVE-2023-6184, CVE-2023-6548, CVE-2023-6549)
Description	Citrix has released security updates addressing multiple vulnerabilities that exists in their products. If exploited these vulnerabilities could lead to Cross-site scripting, remote code execution and Denial of Service It is recommended by Citrix to apply necessary security fixes at earliest to avoid issues
.Affected Products	NetScaler ADC and NetScaler Gateway 14.1 before 14.1-12.35 NetScaler ADC and NetScaler Gateway 13.1 before 13.1-51.15 NetScaler ADC and NetScaler Gateway 13.0 before 13.0-92.21 NetScaler ADC 13.1-FIPS before 13.1-37.176 NetScaler ADC 12.1-FIPS before 12.1-55.302 NetScaler ADC 12.1-NDcPP before 12.1-55.302 Citrix Virtual Apps and Desktops before 2311 Citrix StoreFront before 2308.1 Citrix StoreFront before 2311
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.citrix.com/article/CTX583759/citrix-storefront-security-bulletin-for-cve20235914 https://support.citrix.com/article/CTX583930/citrix-session-recording-security-bulletin-for-cve20236184 https://support.citrix.com/article/CTX584986/netscaler-adc-and-netscaler-gateway-security-bulletin-for-cve20236548-and-cve20236549

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.