Advisory Alert

Alert Number: **AAA20230303** **Date:** **March 3, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SUSE	**High**	Multiple Vulnerabilities
SonicWall	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3112, CVE-2022-3115, CVE-2022-3564, CVE-2022-47520, CVE-2023-23454, CVE-2023-23455)
Description	SUSE has released Security Updates addressing Multiple Linux kernel vulnerabilities. Exploitation of these vulnerabilities can lead to null pointer dereference, use-after-free condition, out of bounds read, type confusion and denial of service. SUSE recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	SUSE Linux Enterprise Micro 5.1 SUSE Linux Enterprise Micro 5.2 SUSE Linux Enterprise Micro for Rancher 5.2 SUSE Linux Enterprise Real Time 15 SP3 SUSE Real Time Module 15-SP3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2023/suse-su-20230591-1/

Affected Product	**SonicWall**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0656, CVE-2023-1101)
Description	SonicWall has released Security Updates addressing multiple vulnerabilities that exist in their products. **CVE-2023-0656** – A Stack based buffer overflow vulnerability exist in the SonicOS, it allows a remote unauthenticated attacker to case Denial of Service. **CVE-2023-1101** – An improper restriction of excessive MFA attempts vulnerability exists in the SonicOS SSLVPN, it allows an authenticated attacker to use excessive MFA codes. SonicWall recommends to apply necessary security fixes at earliest to avoid issues
Affected Products	TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSv 270, NSv 470, NSv 87 version 7.0.1-5095 and earlier versions NSsp 15700 7.0.1-5083 and earlier versions NSv 10, NSv 25, NSv 50, NSv 100, NSv 200, NSv 300, NSv 400, NSv 800, NSv 1600 6.5.4.4-44v-21-1551 and earlier versions NSa 2650, NSa3650, NSa4650, NSa5650, NSa6650, NSa9250, NSa9450, NSa9650 6.5.4.11-97n and earlier versions SOHOW, SOHO 250, SOHO 250W, TZ300, TZ300P, TZ300W, TZ350, TZ350W, TZ400, TZ400W, TZ500, TZ500W, TZ600, TZ600P , NSA 2600, NSA3600, NSA4600, NSA5600, NSA6600, SM9200, SM9400, SM9600, SM9800, SM10200, SM10400, SM10800, NSsp12400, NSsp12800 - 6.5.4.11-97n and earlier versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0005 https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0004

Affected Product	**Ubuntu**
Severity	**High, Medium, Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-3169, CVE-2022-3521, CVE-2022-3344, CVE-2022-3545. CVE-2022-3435, CVE-2022-45869, CVE-2022-47518, CVE-2023-0461, CVE-2022-47519, CVE-2022-4139, CVE-2022-4379, CVE-2022-47521, CVE-2022-47520, CVE-2023-0179, CVE-2022-3565,CVE-2022-43750, CVE-2023-0045, CVE-2022-36879, CVE-2022-20566, CVE-2022-42896, CVE-2022-45934, CVE-2022-3567, CVE-2023-0469, CVE-2022-43945, CVE-2022-47929, CVE-2023-0210, CVE-2022-3707, CVE-2023-23455, CVE-2023-0266, CVE-2022-41218, CVE-2022-36280, CVE-2023-23454, CVE-2022-42703)
Description	Ubuntu has released Security Updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to arbitrary code execution, denial of service and sensitive information disclosure. Ubuntu recommends to apply necessary security fixes at earliest to avoid issues.
Affected Products	Ubuntu 14.04 Ubuntu 22.10 Ubuntu 22.04 Ubuntu 20.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5911-1 https://ubuntu.com/security/notices/USN-5913-1 https://ubuntu.com/security/notices/USN-5914-1 https://ubuntu.com/security/notices/USN-5915-1 https://ubuntu.com/security/notices/USN-5916-1

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.