



Advisory Alert

Alert Number: AAA20230120

Date: January 20, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SonicWALL	High	Path Traversal Vulnerability
Ubuntu	High, Medium, Low	Multiple Vulnerabilities
VMware	Medium	Denial of Service Vulnerability

Description

Affected Product	SonicWALL
Severity	High
Affected Vulnerability	Path Traversal Vulnerability (CVE-2023-0126)
Description	SonicWALL has released a security update addressing a Path Traversal Vulnerability in their products. CVE-2023-0126 - The vulnerability allows an unauthenticated attacker to access arbitrary files and directories stored outside the web root directory of SMA1000 firmware. SonicWALL recommends to apply the necessary fixes at your earliest to avoid issues.
Affected Products	SMA1000 firmware 12.4.2 versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2023-0001

Affected Product	Ubuntu
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-33503, CVE-2022-23521, CVE-2022-41903, CVE-2022-45934, CVE-2022-43945, CVE-2022-3643, CVE-2022-42896, CVE-2022-4378, CVE-2022-3303, CVE-2022-43750, CVE-2022-3646, CVE-2022-4095, CVE-2022-3061, CVE-2022-39842, CVE-2022-20421, CVE-2022-2663, CVE-2022-3586, CVE-2022-40307)
Description	Ubuntu has released a security update addressing Multiple vulnerabilities in their products. If exploited, these vulnerabilities can lead to denial of service and arbitrary code execution. Ubuntu recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Ubuntu 22.10 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-5812-1 https://ubuntu.com/security/notices/USN-5810-2 https://ubuntu.com/security/notices/USN-5813-1 https://ubuntu.com/security/notices/USN-5814-1 https://ubuntu.com/security/notices/USN-5815-1

Affected Product	VMware
Severity	Medium
Affected Vulnerability	Denial of Service Vulnerability (CVE-2022-22938)
Description	VMware has released a security update addressing a Denial of Service vulnerability in their products. CVE-2022-22938 - A denial of service vulnerability exists in VMware Workstation and Horizon Client for Windows caused by an issue in the TrueType font parser. VMware recommends to apply the necessary Security updates at your earliest to avoid issues.
Affected Products	VMware Workstation Pro / Player (Workstation) VMware Horizon Client for Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMMSA-2022-0002.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.