TLP: WHITE

Advisory Alert

Alert Number: **AAA20240719** **Date:** **July 19, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
SolarWinds	**Critical**	Multiple Vulnerabilities
SolarWinds	**High**	Multiple Vulnerabilities
Juniper	**High**	XPath Injection vulnerability
Ivanti	**High**	Path traversal affiliated vulnerability
SonicWall	**High**	Multiple Vulnerabilities

Description

Affected Product	**SolarWinds**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-23471, CVE-2024-23466, CVE-2024-23472, CVE-2024-23469, CVE-2024-23475, CVE-2024-23467)
Description	SolarWinds has released security updates addressing multiple vulnerabilities in SolarWinds Access Rights Manager (ARM). These vulnerabilities can be exploited by authenticated and unauthenticated users to perform remote code execution, arbitrary file deletion, and information disclosure. SolarWinds recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	SolarWinds Access Rights Manager (ARM) 2023.2.4 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23471 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23466 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23472 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23469 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23475 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23467

Affected Product	**SolarWinds**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-28992, CVE-2024-23468, CVE-2024-28993, CVE-2024-23474)
Description	SolarWinds has released security updates addressing multiple vulnerabilities in SolarWinds Access Rights Manager (ARM). These vulnerabilities can be exploited by unauthenticated users to perform arbitrary file deletion and leak sensitive information. SolarWinds recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	SolarWinds Access Rights Manager (ARM) 2023.2.4 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28992 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23468 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-28993 • https://www.solarwinds.com/trust-center/security-advisories/cve-2024-23474

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	XPath Injection vulnerability (CVE-2024-39565)
Description	Juniper has released security update addressing XPath Injection vulnerability that exist in Juniper Networks Junos OS An Improper Neutralization of Data within XPath Expressions ('XPath Injection') vulnerability in J-Web shipped with Juniper Networks Junos OS allows an unauthenticated, network-based attacker to execute remote commands on the target device. While an administrator is logged into a J-Web session or has previously logged in and subsequently logged out of their J-Web session, the attacker can arbitrarily execute commands on the target device with the other user's credentials. In the worst case, the attacker will have full control over the device Juniper recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Junos OS 21.2, 21.4, 22.2, 22.3, 22.4, 23.2, 23.4. Affected platforms: SRX Series, EX Series with J-Web.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-07-Security-Bulletin-Junos-OS-SRX-Series-EX-Series-J-Web-An-unauthenticated-network-based-attacker-can-perform-XPATH-injection-attack-against-a-device-CVE-2024-39565?language=en_US

Affected Product	**Ivanti**
Severity	**High**
Affected Vulnerability	Path traversal affiliated vulnerability (CVE-2024-37403)
Description	Ivanti has released a security update addressing a vulnerability in the Docs@Work for Android application, known as "Dirty Stream." The vulnerability exists due to the application's failure to properly sanitize file names, resulting in a path traversal affiliated vulnerability. This could potentially enable other malicious apps on the device to read sensitive information stored in the app root. Ivanti recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	Ivanti Docs@Work for Android, before 2.26.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://forums.ivanti.com/s/article/Security-Advisory-CVE-2024-37403-Dirty-Stream-for-Ivanti-Docs-Work-for-Android?language=en_US

Affected Product	**SonicWall**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-29014, CVE-2024-40764)
Description	SonicWall has released security updates addressing multiple vulnerabilities in their products. **CVE-2024-29014** - A vulnerability in SonicWall SMA100 NetExtender Windows (32 and 64-bit) client versions 10.2.339 and earlier allows an attacker to execute arbitrary code when processing an EPC Client update. SonicWall strongly advises SSL VPN NetExtender client users to upgrade to the latest release version. This vulnerability does not affect SonicWall firewall (SonicOS) products. **CVE-2024-40764** - A heap-based buffer overflow vulnerability in SonicOS IPSec VPN allows an unauthenticated remote attacker to cause Denial of Service (DoS) in the impacted platforms and versions listed below. SonicWall recommends to apply the necessary security updates at your earliest to avoid issues.
Affected Products	NetExtender Windows (32 and 64 bit) 10.2.339 and earlier versions. **Gen6 NSv** - NSv10, NSv25, NSv50, NSv100, NSv200, NSv300, NSv400, NSv800, NSv1600 - 6.5.4.4-44v-21-2395 and older versions **Gen7** - 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, NSsp 15700 NSv 270, NSv 470, NSv 870 7.0.1-5151 and older versions and 7.1.1-7051 and older versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0011 • https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2024-0012

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.