Advisory Alert

Alert Number: AAA20240701 **Date:** July 1, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Juniper	**Critical**	Authentication Bypass Vulnerability
IBM	**High**, Medium	Multiple Vulnerabilities
NetApp	**High**, Medium	Multiple Vulnerabilities
Dell	**High**, Low	Multiple Vulnerabilities

Description

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Authentication Bypass Vulnerability (CVE-2024-2973)
Description	Juniper has released security updates addressing an Authentication Bypass Vulnerability that exists in Juniper Networking devices. An Authentication Bypass Using an Alternate Path or Channel vulnerability in Juniper Networks Session Smart Router or Conductor running with a redundant peer allows a network based attacker to bypass authentication and take full control of the device. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Below Routers and Conductors that are running in high-availability redundant configurations are affected by this vulnerability. Session Smart Router: • All versions before 5.6.15 • From 6.0 before 6.1.9-lts • From 6.2 before 6.2.5-sts Session Smart Conductor: • All versions before 5.6.15 • From 6.0 before 6.1.9-lts • From 6.2 before 6.2.5-sts WAN Assurance Router: • 6.0 versions before 6.1.9-lts • 6.2 versions before 6.2.5-sts
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-06-Out-Of-Cycle-Security-Bulletin-Session-Smart-Router-SSR-On-redundant-router-deployments-API-authentication-can-be-bypassed-CVE-2024-2973?language=en_US

Affected Product	**IBM**
Severity	**High**, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-23807, CVE-2024-22329, CVE-2024-25026)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in IBM Storage Protect for Space Management. **CVE-2024-23807** - Apache Xerces C++ XML parser could allow a remote attacker to execute arbitrary code on the system, caused by a use-after-free flaw during the scanning of external DTDs. By sending a specially crafted request, an attacker could exploit this vulnerability to execute arbitrary code on the system. **CVE-2024-22329** - IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.3 are vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, an attacker could exploit this vulnerability to conduct the SSRF attack. **CVE-2024-25026** - IBM WebSphere Application Server 8.5, 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 24.0.0.4 are vulnerable to a denial of service, caused by sending a specially crafted request. A remote attacker could exploit this vulnerability to cause the server to consume memory resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Protect for Space Management versions 8.1.0.0 - 8.1.22.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7159097

Affected Product	**NetApp**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-3454, CVE-2024-2859, CVE-2023-5973)
Description	NetApp has released security updates addressing multiple Vulnerabilities that exist in their products. **CVE-2023-3454** - Remote code execution (RCE) vulnerability in Brocade Fabric OS after v9.0 and before v9.2.0 could allow an attacker to execute arbitrary code and use this to gain root access to the Brocade switch. **CVE-2024-2859** - By default, SANnav OVA is shipped with root user login enabled. While protected by a password, access to root could expose SANnav to a remote attacker should they gain access to the root account. **CVE-2023-5973** - Brocade Web Interface in Brocade Fabric OS v9.x and before v9.2.0 does not properly represent the portName to the user if the portName contains reserved characters. This could allow an authenticated user to alter the UI of the Brocade Switch and change ports display. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Brocade Fabric OS versions v9.0 prior to v9.2.0 Brocade SANnav OVA versions prior to v2.3.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20240628-0004/ • https://security.netapp.com/advisory/ntap-20240628-0003/ • https://security.netapp.com/advisory/ntap-20240628-0005/

Affected Product	**Dell**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-29499, CVE-2024-25943, CVE-2024-3411, CVE-2024-37137)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC9 14th Generation: versions prior to 7.00.00.172 iDRAC9 15th and 16th Generations: versions prior to 7.10.50.00 iDRAC8 13th Generation versions prior to 2.86.86.86 iDRAC9 firmware versions prior to 7.10.50.00 on Precision 7960 and Precision 7960 XL Racks iDRAC9 firmware versions prior to 7.00.00.172 on Precision 7920 and 7920 XL Racks Dell CloudLink versions prior to 7.1.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000222769/dsa-2024-013-security-update-for-dell-precision-rack-for-an-idrac9-vulnerability • https://www.dell.com/support/kbdoc/en-us/000226503/dsa-2024-099-security-update-for-dell-idrac9-ipmi-session-vulnerability • https://www.dell.com/support/kbdoc/en-us/000226504/dsa-2024-295-security-update-for-dell-idrac8-ipmi-session-vulnerability • https://www.dell.com/support/kbdoc/en-us/000226476/dsa-2024-294-security-update-for-dell-cloudlink-vulnerability

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.