Advisory Alert

Alert Number: AAA20240830 **Date:** August 30, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Juniper	**Critical**	Multiple Vulnerabilities
IBM	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
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	Dell RecoverPoint for Virtual Machines - Version 6.0.SP1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000228154/dsa-2024-369-security-update-for-dell-recoverpoint-for-virtual-machines-multiple-vulnerabilities

Affected Product	**Juniper**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-35116, CVE-2023-34453, CVE-2023-34455, CVE-2023-34454, CVE-2023-43642, CVE-2023-2976, CVE-2023-33201, CVE-2023-46136, CVE-2023-43804, CVE-2023-37920, CVE-2022-25883, CVE-2023-45133, CVE-2023-31484, CVE-2023-1370, CVE-2021-4048, CVE-2021-23445, CVE-2021-31684, CVE-2023-38019, CVE-2023-38020, CVE-2023-38263, CVE-2023-46308, CVE-2023-32006, CVE-2023-32002, CVE-2023-32559, CVE-2022-38900, CVE-2023-45857, CVE-2022-25927, CVE-2023-44270, CVE-2023-26159, CVE-2020-19909, CVE-2023-38546, CVE-2023-38545, CVE-2023-5678, CVE-2023-46218, CVE-2023-46219, CVE-2023-4807, CVE-2023-0727, CVE-2023-6129, CVE-2023-5363, CVE-2022-21216, CVE-2023-46234, CVE-2024-28849, CVE-2024-29041, CVE-2024-29180, CVE-2024-4067, CVE-2024-4068, CVE-2024-21501, CVE-2024-27088, CVE-2024-27982, CVE-2024-27983)
Description	Juniper has issued security updates addressing multiple vulnerabilities that exist in Juniper Networks Juniper Secure Analytics Applications. If Exploited, these vulnerabilities could lead to Denial of Service, Remote Code Execution, Disclosure of Information. Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Juniper Networks Juniper Secure Analytics: • Log Collector Application prior to version v1.8.4 • SOAR Plugin Application prior to version 5.3.1 • Deployment Intelligence Application prior to 3.0.13 • User Behavior Analytics Application add-on prior to 4.1.14 • Pulse Application add-on prior to 2.2.12 • Assistant Application add-on prior to 3.6.0 • Use Case Manager Application add-on prior to 3.9.0 • WinCollect Standalone Agent prior to 10.1.8 • M7 Appliances prior to 4.0.0 • Log Source Management App prior to 7.0.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-01-Security-Bulletin-JSA-Series-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US

Affected Product	**IBM**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-3933, CVE-2024-21094, CVE-2024-21085, CVE-2024-21011, CVE-2023-38264)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause denial of service, security restriction bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM WebSphere eXtreme Scale - Version 8.6.1.0 - 8.6.1.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7166876

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.