Advisory Alert

Alert Number: AAA20241104 **Date:** November 4, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
IBM	**Critical**	Integer Overflow and Buffer Overflow Vulnerabilities
Juniper	**Critical**	Multiple Vulnerabilities
Qnap	**Critical**	Security Update
IBM	**High**, **Medium**, **Low**	Multiple Vulnerabilities
Ubuntu	**Medium**	Multiple Vulnerabilities
NetApp	**Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**IBM**
Severity	**Critical**
Affected Vulnerability	Integer Overflow and Buffer Overflow Vulnerabilities (CVE-2020-36242)
Description	IBM has released security updates addressing an Integer Overflow Vulnerability and a Buffer Overflow Vulnerability that exist in IBM QRadar SIEM. **CVE-2020-36242** - Cryptography could allow a remote attacker to execute arbitrary code on the system, caused by an integer overflow and a buffer overflow. By using certain sequences of update calls to symmetrically encrypt multi-GB values, a remote attacker could exploit this vulnerability to execute arbitrary code on the system or cause a denial of service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7174634

Affected Product	**Juniper**
Severity	**Critical** - Initial release date **8th February 2024 (AAA20240208)**
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, CVE-2021-23727, CVE-2024-39338, CVE-2019-13224, CVE-2019-16163, CVE-2019-19012, CVE-2022-24735, CVE-2022-24736, CVE-2022-24834, CVE-2023-28856, CVE-2023-45145)
Description	Juniper has released security updates addressing multiple vulnerabilities that exist in Juniper Secure Analytics optional Applications. These vulnerabilities could be exploited by malicious users to cause Denial of Service, Fatal Errors, Directory traversal, Information Disclosure, Authentication Bypass. 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 3.0.14 • 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 3.8.0 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/On-Demand-JSA-Series-Multiple-vulnerabilities-resolved-in-JSA-Applications?language=en_US

Affected Product	**Qnap**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2024-50387)
Description	Qnap has released security updates addressing a vulnerability that exists in SMB Service. This vulnerability could be exploited by malicious users to compromise the affected system. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	SMB Service 4.15.x SMB Service h4.15.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.qnap.com/en/security-advisory/qsa-24-42

Affected Product	**IBM**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Information Disclosure, Cross-site Scripting, Arbitrary Code Execution, Denial Of Service. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM QRadar SIEM versions 7.5 - 7.5.0 UP10 WebSphere Service Registry and Repository version 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7174634 • https://www.ibm.com/support/pages/node/7174638 • https://www.ibm.com/support/pages/node/7174636 • https://www.ibm.com/support/pages/node/7174637

Affected Product	**Ubuntu**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. These vulnerabilities could be exploited by malicious users to compromise the affected system. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7089-1

Affected Product	**NetApp**
Severity	**Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26733, CVE-2024-26735, CVE-2024-21247)
Description	NetApp has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-26733** - Multiple NetApp products incorporate Linux kernel. Certain versions of Linux kernel are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service. **CVE-2024-26735** - Multiple NetApp products incorporate Linux kernel. Certain versions of Linux kernel are susceptible to a vulnerability which when successfully exploited could lead to Denial of Service. **CVE-2024-21247** - Multiple NetApp products incorporate Oracle MySQL Client. MySQL Client versions through 8.0.39, through 8.4.2, and through 9.0.1 are susceptible to a vulnerability that can result in unauthorized update, insert or delete access to some of MySQL Client accessible data as well as unauthorized read access to a subset of MySQL Client accessible data. NetApp advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	E-Series SANtricity OS Controller Software 11.x OnCommand Workflow Automation Active IQ Unified Manager SnapCenter Server
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://security.netapp.com/advisory/ntap-20241101-0013/ • https://security.netapp.com/advisory/ntap-20241101-0012/ • https://security.netapp.com/advisory/ntap-20241101-0006/

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.