Advisory Alert

Alert Number: AAA20240402 **Date:** April 2, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
IBM	**High**, **Medium**	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. Malicious users may exploit these vulnerabilities, which could compromise the affected system. Dell recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell EMC VxRail Appliance - 8.0.x versions prior to 8.0.120
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000223698/dsa-2023-440-security-update-for-dell-vxrail-multiple-third-party-component-vulnerabilities-8-0-120

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-44487, CVE-2023-50313, CVE-2023-44483)
Description	IBM has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2023-44487**- Multiple vendors are vulnerable to a denial of service, caused by a flaw in handling multiplexed streams in the HTTP/2 protocol. By sending numerous HTTP/2 requests and RST_STREAM frames over multiple streams, a remote attacker could exploit this vulnerability to cause a denial of service due to server resource consumption. **CVE-2023-50313** - IBM WebSphere Application Server could provide weaker than expected security for outbound TLS connections caused by a failure to honor user configuration. **CVE-2023-44483** - Apache Santuario could allow a remote authenticated attacker to obtain sensitive information, caused by the storage of a private key in the log files when using the JSR 105 API. By gaining access to the log files, an attacker could exploit this vulnerability to obtain the private key information, and use this information to launch further attacks against the affected system. IBM recommends to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Tivoli Netcool Impact - Version 7.1.0.0 - 7.1.0.32 IBM WebSphere Application Server - Version 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7145620 • https://www.ibm.com/support/pages/node/7145607 • https://www.ibm.com/support/pages/node/7145606

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.