Advisory Alert

Alert Number: AAA20240312 **Date:** March 12, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

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

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-48795, CVE-2023-38408, CVE-2023-5344, CVE-2023-23583)
Description	Dell has issued security updates addressing multiple vulnerabilities that exist in Dell NetWorker vProxy components. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at earliest to avoid problems.
Affected Products	NetWorker vProxy OVA v19.9 - v19.9.0.4 NetWorker vProxy OVA v19.8 - v19.8.0.4 NetWorker vProxy OVA v19.8 and prior versions
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222965/dsa-2024-091-security-update-for-dell-networker-vproxy-multiple-component-vulnerabilities

Affected Product	**Dell**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-20932, CVE-2024-20918, CVE-2024-20952, CVE-2024-20919, CVE-2024-20921, CVE-2024-20926, CVE-2024-20945, CVE-2024-20923, CVE-2024-20925, CVE-2024-20922, CVE-2022-21166)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in Dell NRE and Networking firmware. These vulnerabilities could be exploited by malicious users to gain access, modify critical data and enabling information disclosure. Dell recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	Dell NetWorker Runtime Environment (NRE) v8.0.19 Dell Networking Z9332F-ON Versions prior to v1.1.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000222962/dsa-2023-126-security-update-for-dell-networker-runtime-environment-nre-oracle-java-se-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000222981/dsa-2024-117-security-update-for-dell-networking-z9332f-on-for-third-party-vulnerabilities

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-22195, CVE-2024-26130, CVE-2023-50782)
Description	IBM has released security updates addressing multiple vulnerabilities in IBM Storage Defender. If exploited, these vulnerabilities could lead to Denial of Service, sensitive information disclosure and Cross-Site Scripting. **CVE-2024-22195** - Jinja is an extensible templating engine. Special placeholders in the template allow writing code similar to Python syntax. It is possible to inject arbitrary HTML attributes into the rendered HTML template, potentially leading to Cross-Site Scripting (XSS). **CVE-2024-26130** - cryptography is vulnerable to a denial of service, caused by a NULL pointer dereference in the pkcs12.serialize_key_and_certificates process. By sending a specially crafted request, a remote attacker could exploit this vulnerability to cause a denial of service. **CVE-2023-50782** - A flaw was found in the python-cryptography package. This issue may allow a remote attacker to decrypt captured messages in TLS servers that use RSA key exchanges, which may lead to exposure of confidential or sensitive data. IBM recommends to apply the necessary patch updates at your earliest to avoid issues.
Affected Products	IBM Storage Defender - Resiliency Service v2.0.0 - v2.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.ibm.com/support/pages/node/7129823

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-4244, CVE-2023-46838, CVE-2023-50431, CVE-2023-51779, CVE-2023-51780, CVE-2023-51782, CVE-2023-52436, CVE-2023-52438, CVE-2023-52439, CVE-2023-52443, CVE-2023-52444, CVE-2023-52445, CVE-2023-52447, CVE-2023-52448, CVE-2023-52449, CVE-2023-52451, CVE-2023-52454, CVE-2023-52456, CVE-2023-52457, CVE-2023-52458, CVE-2023-52462, CVE-2023-52463, CVE-2023-52464, CVE-2023-52467, CVE-2023-52469, CVE-2023-52470, CVE-2023-52583, CVE-2023-52584, CVE-2023-52587, CVE-2023-52588, CVE-2023-52589, CVE-2023-52593, CVE-2023-52594, CVE-2023-52595, CVE-2023-52597, CVE-2023-52598, CVE-2023-52599, CVE-2023-52600, CVE-2023-52601, CVE-2023-52602, CVE-2023-52603, CVE-2023-52604, CVE-2023-52605, CVE-2023-52606, CVE-2023-52607, CVE-2023-52602, CVE-2023-5633, CVE-2023-6121, CVE-2023-6610, CVE-2023-6932, CVE-2024-0340, CVE-2024-1085, CVE-2024-1086, CVE-2024-23849, CVE-2024-24860, CVE-2024-26581, CVE-2024-26588, CVE-2024-26589, CVE-2024-26591, CVE-2024-26592, CVE-2024-26594, CVE-2024-26597, CVE-2024-26598, CVE-2024-26599, CVE-2024-26600, CVE-2024-26601, CVE-2024-26624, CVE-2024-26625, CVE-2024-26627, CVE-2024-26628)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. If exploited, these could allow a local attacker to cause Denial of Service, sensitive Information disclosure and arbitrary code execution. It is recommended by Ubuntu to apply necessary security fixes at your earliest to avoid issues.
.Affected Products	Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6688-1 https://ubuntu.com/security/notices/USN-6681-2

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.