# Advisory Alert

**Alert Number:** AAA20230515 **Date:** May 15, 2023

**Document Classification Level :** Public Circulation Permitted | Public

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Dell** | **Critical** | **Multiple Vulnerabilities** |
| **PostgreSQL** | **High , Medium** | Multiple Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities (CVE-2022-37436, CVE-2022-36760, CVE-2006-20001, CVE-2018-25032, CVE-2019-10086, CVE-2020-10683, CVE-2020-11022, CVE-2020-36518, CVE-2021-0153, CVE-2021-0154, CVE-2021-0155, CVE-2021-0190, CVE-2021-33123, CVE-2021-33124, CVE-2021-3426, CVE-2021-36090, CVE-2021-3918, CVE-2021-4104, CVE-2021-43859, CVE-2021-44228 , CVE-2021-44790, CVE-2021-44832, CVE-2021-45046, CVE-2021-45105, CVE-2022-0778, CVE-2022-1292, CVE-2022-2068, CVE-2022-21166, CVE-2022-21636, CVE-2022-22971, CVE-2022-22978, CVE-2022-23181, CVE-2022-23218, CVE-2022-23219, CVE-2022-23305, CVE-2022-23437, CVE-2022-23943, CVE-2022-25315, CVE-2022-29824, CVE-2022-29885, CVE-2022-31813, CVE-2022-34305, CVE-2022-35737) |
| Description | Dell has released security updates to address multiple third party vulnerabilities in Dell RecoverPoint Classic and Dell NetWorker Management Console (NMC). If exploited, these vulnerabilities could lead to HTTP request smuggling, denial of service, HTTP response splitting, and remote code execution.<br><br>Dell highly recommends to apply necessary security fixes at earliest to avoid issues. |
| Affected Products | Dell NetWorker Management Console (NMC) 19.7.0.3 and prior releases<br>Dell NetWorker Management Console (NMC) 19.8.0.1 and prior releases<br>Dell NetWorker Management Console (NMC) 19.7.1<br>RecoverPoint Classic 5.1 SP4, 5.1 SP4 P1, 5.1 SP4 P2, 5.1 SP4 P3 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000213385/dsa-2023-054-dell-networker-management-console-nmc-security-update-for-multiple-vulnerabilities<br>https://www.dell.com/support/kbdoc/en-us/000213384/dsa-2023-169-dell-recoverpoint-classic-security-update-for-multiple-component-vulnerabilities |

| | |
|---|---|
| Affected Product | **PostgreSQL** |
| Severity | **High , Medium** |
| Affected Vulnerability | Multiple vulnerabilities (CVE-2023-2454, CVE-2023-2455) |
| Description | PostgreSQL has released a patch update addressing multiple vulnerabilities in PostgreSQL versions 11 to 15.<br><br>**CVE-2023-2454 -** An arbitrary code execution vulnerability exists due to improperly imposed security restrictions. An attacker with database-level CREATE privilege can execute arbitrary code as the bootstrap superuser.<br><br>**CVE-2023-2455 -** Security features bypass vulnerability involving function inlining in databases that have used CREATE POLICY to define a row security policy. Applying an incorrect policy may permit a user to complete otherwise-forbidden reads and modifications.<br><br>PostgreSQL recommends to apply necessary security fixes at earliest to avoid issues |
| Affected Products | PostgreSQL version 11 to version 15 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.postgresql.org/about/news/postgresql-153-148-1311-1215-and-1120-released-2637/ |

## 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.**