# Advisory Alert

**Alert Number:** AAA20221115 **Date:** November 15, 2022

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Ubuntu** | Medium, Low | Multiple Vulnerabilities |
| **Dell** | Low | Improper Input Validation Vulnerabilities |

## Description

| | |
|---|---|
| Affected Product | **Ubuntu** |
| Severity | Medium, Low |
| Affected Vulnerability | Multiple Vulnerabilities(CVE-2022-1674, CVE-2022-2125, CVE-2022-2304, CVE-2022-1725, CVE-2022-2124, CVE-2022-2126, CVE-2022-2183, CVE-2022-2175, CVE-2022-2206) |
| Description | Ubuntu has released a security update addressing multiple vulnerabilities that exist in the vim editor that's used in the Ubuntu. If exploited these vulnerabilities could cause denial of service and arbitrary command execution.<br><br>Ubuntu highly recommends to apply the available patch updates at your earliest to avoid issues. |
| Affected Products | Ubuntu 16.04 vim package versions before 2:7.4.1689-3ubuntu1.5+esm13 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://ubuntu.com/security/notices/USN-5723-1 |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | Low |
| Affected Vulnerability | Improper Input Validation Vulnerabilities(CVE-2022-34435, CVE-2022-34436) |
| Description | Dell has released a security update addressing multiple Input validation vulnerabilities that exist in their products.<br><br>**CVE-2022-34435 –** An improper input validation vulnerability that exist in the Dell iDRAC9 version 6.00.02.00 and prior versions Racadm when the firmware lock-down configuration is set. A remote high privileged attacker can use this to bypass the firmware lock-down configuration and perform a firmware update.<br><br>**CVE-2022-34436** - An improper input validation vulnerability that exist in the Dell iDRAC8 version 2.83.83.83 and prior versions Racadm when the firmware lock-down configuration is set. A remote high privileged attacker can use this to bypass the firmware lock-down configuration and perform a firmware update.<br><br>Dell highly recommends to apply the available patch updates at your earliest to avoid issues. |
| Affected Products | Dell iDRAC9 versions before 6.00.30.00<br>Dell iDRAC8 Versions before 2.84.84.84 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000205346/dsa-2022-265-dell-idrac8-and-dell-idrac9-security-update-for-a-racadm-vulnerability |

### 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.**