# Advisory Alert

**Alert Number:** AAA20231012 **Date:** October 12, 2023

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

**Information Classification Level :** TLP: WHITE

## Overview

| Product | Severity | Vulnerability |
|---|---|---|
| **Fortinet** | **Critical** | Relative path traversal vulnerability |
| **Dell** | **Critical** | Multiple Vulnerabilities |
| **Dell** | **High** | Improper Access Control vulnerability |
| **Palo Alto** | **Medium** | Sensitive information disclosure Vulnerability |

## Description

| | |
|---|---|
| Affected Product | **Fortinet** |
| Severity | **Critical** |
| Affected Vulnerability | Relative path traversal vulnerability (CVE-2023-40714) |
| Description | Fortinet has released a critical security update for FortiSIEM addressing a relative path traversal vulnerability in file upload components which may allow an authenticated, low privileged user of the FortiSIEM GUI to escalate their privilege and replace arbitrary files on the underlying filesystem via specifically crafted HTTP requests.<br><br>Fortinet recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | FortiSIEM version 7.0.0<br>FortiSIEM version 6.7.0 through 6.7.3<br>FortiSIEM version 6.6.0 through 6.6.3<br>FortiSIEM version 6.5.0 through 6.5.1<br>FortiSIEM version 6.4.0 through 6.4.2 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.fortiguard.com/psirt/FG-IR-23-085 |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **Critical** |
| Affected Vulnerability | Multiple Vulnerabilities |
| Description | Dell has released security updates addressing multiple vulnerabilities. Exploitation of the most severe vulnerabilities could lead to heap out-of-bounds write, privilege escalation, sensitive information disclosure and compromise the affected system.<br><br>Dell recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Dell EMC VxRail Appliance Versions prior to 8.0.020 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000210980/dsa-2023-065-dell-vxrail-8-x-security-update-for-multiple-third-party-component-vulnerabilities<br>https://www.dell.com/support/kbdoc/en-us/000213011/dsa-2023-071-dell-vxrail-security-update-for-multiple-third-party-component-vulnerabilities-7-0-450 |

| | |
|---|---|
| Affected Product | **Dell** |
| Severity | **High** |
| Affected Vulnerability | Improper Access Control vulnerability (CVE-2023-43079) |
| Description | Dell has released a security updates addressing an Improper Access Control vulnerability in Dell OpenManage Server Administrator. A local low-privileged malicious user could potentially exploit this vulnerability to execute arbitrary code in order to elevate privileges on the system. |
| Affected Products | Dell OpenManage Server Administrator versions 11.0.0.0 and prior<br>Dell Systems Management Tools and Documentation DVD ISO versions 11.0.0.0 and prior |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://www.dell.com/support/kbdoc/en-us/000218469/dsa-2023-367-dell-openmanage-server-administrator-omsa-security-update-for-multiple-vulnerabilities |

| | |
|---|---|
| Affected Product | **Palo Alto** |
| Severity | **Medium** |
| Affected Vulnerability | Sensitive information disclosure Vulnerability (CVE-2023-3281) |
| Description | Palo Alto has released security update addressing Cleartext Exposure of Client Certificate Key in Kafka v3 Integration.Palo Alto recommends to apply the necessary patch updates at your earliest to avoid issues. |
| Affected Products | Cortex XSOAR Kafka Integration v3 below version 2.0.16 |
| Officially Acknowledged by the Vendor | Yes |
| Patch/ Workaround Released | Yes |
| Reference | https://security.paloaltonetworks.com/CVE-2023-3281 |

**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.**