TLP: WHITE

Advisory Alert

Alert Number: **AAA20230927** **Date:** **September 27, 2023**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities
VMware	**Medium**	Local Privilege Escalation Vulnerability

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead Information Disclosure, Out of Bounds write, Privilege escalation and compromise the affected system. Dell highly recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Dell Avamar Data Store Gen5a with BIOS version prior to 2.18.1 Dell EMC VPlex Metro Node Versions prior to 8.0.0 Dell EMC VPlex Metro BIOS Versions prior to 2.17.1 Dell EMC VPlex Metro iDRAC Versions prior to 6.10.30.20 Dell EMC VPlex Metro NIC Versions prior to 21.5.9
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000218008/dsa-2023-114-security-update-for-dell-avamar-data-store-gen5a-vulnerabilities https://www.dell.com/support/kbdoc/en-us/000217979/dsa-2023-281-security-update-for-dell-emc-vplex-metro-node-multiple-third-party-component-vulnerabilities

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-27672, CVE-2022-40982, CVE-2023-3863, CVE-2023-3212, CVE-2023-40283, CVE-2023-4128, CVE-2023-2002, CVE-2023-35828, CVE-2023-3268, CVE-2023-2269, CVE-2023-35824, CVE-2023-35823, CVE-2023-3609, CVE-2023-31084, CVE-2023-3776, CVE-2023-2163, CVE-2023-21255, CVE-2023-3611, CVE-2023-20593, CVE-2023-20588)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities could lead to sensitive Information disclosure, denial of service, arbitrary code execution Ubuntu recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	Ubuntu 20.04 Ubuntu 18.04 Ubuntu 16.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-6396-1 https://ubuntu.com/security/notices/USN-6397-1 https://ubuntu.com/security/notices/USN-6387-2

Affected Product	**VMware**
Severity	**Medium**
Affected Vulnerability	Local Privilege Escalation Vulnerability (CVE-2023-34043)
Description	VMware has released a security update addressing Local Privilege Escalation Vulnerability exist in VMware Aria Operations. By exploiting this a malicious actor with administrative access to the local system can escalate privileges to 'root'. VMware recommends to apply the necessary security updates at earliest to avoid issues
Affected Products	VMware Aria Operations version 8.12.x VMware Aria Operations version 8.10.x VMware Aria Operations version 8.6.x VMware Cloud Foundation (VMware Aria Operations) version 5.x VMware Cloud Foundation (VMware Aria Operations) version 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.vmware.com/security/advisories/VMSA-2023-0020.html

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.