Advisory Alert

Alert Number: AAA20230724 **Date:** July 24, 2023

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**High**	Multiple Vulnerabilities
Lenovo	**High**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-20896, CVE-2023-20895, CVE-2023-20894, CVE-2023-20893, CVE-2023-20892 CVE-2023-32324, CVE-2023-32067, CVE-2023-31147, CVE-2023-31130, CVE-2023-31124, CVE-2023-30772, CVE-2023-30630, CVE-2023-29469, CVE-2023-29383, CVE-2023-28772, CVE-2023-28708, CVE-2023-28642, CVE-2023-28487, CVE-2023-28486, CVE-2023-28484, CVE-2023-28466, CVE-2023-28464, CVE-2023-28328, CVE-2023-28327, CVE-2023-28322, CVE-2023-28321, CVE-2023-28320, CVE-2023-27561, CVE-2023-26545, CVE-2023-2650, CVE-2023-25809, CVE-2023-25193, CVE-2023-25012, CVE-2023-24998, CVE-2023-2455, CVE-2023-2454, CVE-2023-24329, CVE-2023-23559, CVE-2023-23006, CVE-2023-23004, CVE-2023-23000, CVE-2023-22995, CVE-2023-21968, CVE-2023-21967, CVE-2023-21954, CVE-2023-21939, CVE-2023-21938, CVE-2023-21937, CVE-2023-21930, CVE-2023-21843, CVE-2023-21835, CVE-2023-2176, CVE-2023-2162, CVE-2023-2008, CVE-2023-1998, CVE-2023-1990CVE-2023-1989, CVE-2023-1872, CVE-2023-1855, CVE-2023-1838, CVE-2023-1670, CVE-2023-1611, CVE-2023-1582, CVE-2023-1513, CVE-2023-1390, CVE-2023-1382, CVE-2023-1281, CVE-2023-1195, CVE-2023-1175, CVE-2023-1170, CVE-2023-1127, CVE-2023-1118, CVE-2023-1095, CVE-2023-1078, CVE-2023-1076, CVE-2023-1075, CVE-2023-0922, CVE-2023-0597, CVE-2023-0590, CVE-2023-0512, CVE-2023-0466, CVE-2023-0465, CVE-2023-0464, CVE-2023-0461, CVE-2023-0394, CVE-2023-0045, CVE-2022-4904, CVE-2022-4744, CVE-2022-45143, CVE-2022-43945, CVE-2022-41862, CVE-2022-38096, CVE-2022-36280, CVE-2022-36109, CVE-2022-29824, CVE-2022-28737, CVE-2022-23471, CVE-2022-2196, CVE-2021-3923, CVE-2021-3541, CVE-2021-30560, CVE-2021-30465, CVE-2020-36691, CVE-2020-36242, CVE-2020-25659, CVE-2019-20916, CVE-2019-19921, CVE-2019-15133, CVE-2018-11490, CVE-2017-5753, CVE-2016-3977)
Description	Dell has released a security update to address multiple vulnerabilities in Dell EMC VxRail Appliance These vulnerabilities may result in a denial-of-service, out-of-bounds read, heap buffer overflow Dell recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	Dell EMC VxRail Appliance Prior to Version 7.0.452
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000216008/dsa-2023-257-security-update-for-dell-vxrail-vulnerabilities

Affected Product	**Lenovo**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-34329, CVE-2023-34330)
Description	Lenovo has released a security updates addressing authentication bypass and code execution Vulnerabilities in Dell Baseboard Management Controller (BMC) – ThinkSystem. By combining these vulnerabilities, a remote attacker with network access to the BMC management interface and lacking BMC credentials can gain remote code execution on servers running vulnerable firmware. Lenovo recommends to apply the necessary security fixes at your earliest to avoid issues.
Affected Products	HR610X (Hyperscale)-Baseboard Management Controller (BMC) - ThinkSystem HR610X versions before 15.40 HR630X (HyperScale)-Baseboard Management Controller (BMC) - ThinkSystem HR630X/HR650X versions before 11.53 HR630X V2 (Hyperscale) Baseboard Management Controller (BMC) - ThinkSystem HR630X_V2 versions before 1.52 HR650X (Hyperscale) Baseboard Management Controller (BMC) - ThinkSystem HR630X/HR650X versions before11.53
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.lenovo.com/us/en/product_security/LEN-125170

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.