Advisory Alert

Alert Number: AAA20240627 **Date:** June 27, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Hitachi	**High**	Multiple Vulnerabilities
Dell	**Medium**	OpenSSH Terrapin attack
VMware Broadcom	**Medium**	Multiple vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-0172, CVE-2022-40982, CVE-2022-43505, CVE-2024-0154, CVE-2024-0173, CVE-2024-0161, CVE-2023-39432, CVE-2023-33870, CVE-2023-29153, CVE-2023-47165, CVE-2024-21828, CVE-2021-3711, CVE-2021-3712, CVE-2022-0778, CVE-2020-8670, CVE-2022-21233, CVE-2022-26074, CVE-2021-33060, CVE-2021-28216, CVE-2022-21198, CVE-2022-26845, CVE-2022-29893, CVE-2022-27497, CVE-2022-33159, CVE-2022-26343, CVE-2022-26006, CVE-2021-0187, CVE-2022-26837, CVE-2022-29466, CVE-2022-29515, CVE-2021-30004, CVE-2022-36372, CVE-2017-5715, CVE-2023-0215, CVE-2022-4450, CVE-2023-0286, CVE-2022-4304, CVE-2021-38578)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in multiple third party products which are use in Dell Avamar, Dell Integrated Data Protection Appliance. These vulnerabilities could be exploited by malicious users to compromise the affected system. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Avamar Data Store Gen5A running on Dell Avamar operating system version ADS Gen5A Dell Avamar Data Store Gen4T running on Dell Avamar operating system version ADS Gen4T Dell Power Protect DP Series (Integrated Data Protection Appliance (IDPA)) running on Dell Avamar operating system Version 2.7.6 and prior (only 8x Models)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000226426/dsa-2024-250-security-update-for-dell-avamar-dell-integrated-data-protection-appliance-idpa-security-update-for-multiple-vulnerabilities

Affected Product	**Hitachi**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-28746, CVE-2024-21407, CVE-2024-21408, CVE-2024-21427, CVE-2024-21429, CVE-2024-21430, CVE-2024-21431, CVE-2024-21432, CVE-2024-21433, CVE-2024-21434, CVE-2024-21436, CVE-2024-21437, CVE-2024-21438, CVE-2024-21439, CVE-2024-21440, CVE-2024-21441, CVE-2024-21442, CVE-2024-21443, CVE-2024-21444, CVE-2024-21445, CVE-2024-21446, CVE-2024-21450, CVE-2024-21451, CVE-2024-26159, CVE-2024-26161, CVE-2024-26162, CVE-2024-26166, CVE-2024-26169, CVE-2024-26170, CVE-2024-26173, CVE-2024-26174, CVE-2024-26176, CVE-2024-26177, CVE-2024-26178, CVE-2024-26181, CVE-2024-26182)
Description	Hitachi has released security updates addressing multiple vulnerabilities that exist in third party components which affects Hitachi Disk Array Systems. These vulnerabilities could be exploited by malicious users to cause Kernel Information Disclosure, Kernel Elevation of Privilege, Kernel Denial of Service, Remote Code Execution. Hitachi advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Hitachi Virtual Storage Platform 5200, 5600, 5200H, 5600H, 5100, 5500, 5100H, 5500H Hitachi Virtual Storage Platform G1000, G1500 Hitachi Virtual Storage Platform F1500 Hitachi Virtual Storage Platform VX7
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.hitachi.com/products/it/storage-solutions/sec_info/2024/03.html#vuln

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	OpenSSH Terrapin attack (CVE-2023-48795)
Description	Dell has released a security update addressing the OpenSSH Terrapin attack, which affects iDRAC 8 and iDRAC 9. By exploiting remote attackers to bypass integrity checks, some packets are omitted, and a client and server may consequently end up with a connection for which some security features have been downgraded or disabled. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	iDRAC 9 Versions prior to 7.00.00.171 for 14th Generation PowerEdge Rx4xx/ Cx4xx iDRAC 9 Versions prior to 7.10.30.05 for 16th Generation PowerEdge Rx6xx iDRAC 9 Versions prior to 7.10.50.00 for 15th and 16th Generation PowerEdge iDRAC 8 Versions prior to 2.86.86.86 for 13th Generation PowerEdge
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000221558/dsa-2024-021-idrac-8-and-idrac-9-security-update-for-cve-2023-48795

Affected Product	**VMware Broadcom**
Severity	**Medium**
Affected Vulnerability	Multiple vulnerabilities (CVE-2024-37085, CVE-2024-37086, CVE-2024-37087)
Description	Broadcom has released a security update addressing multiple vulnerabilities that exist in VMware products. **CVE-2024-37085 -** VMware ESXi contains an authentication bypass vulnerability. malicious actor with sufficient Active Directory (AD) permissions can gain full access to an ESXi host that was previously configured to use AD for user management by re-creating the configured AD group ('ESXi Admins' by default) after it was deleted from AD. **CVE-2024-37086 -** VMware ESXi contains an out-of-bounds read vulnerability .A malicious actor with local administrative privileges on a virtual machine with an existing snapshot may trigger an out-of-bounds read leading to a denial-of-service condition of the host. **CVE-2024-37087 -** A malicious actor with network access to vCenter Server may create a denial-of-service condition Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware ESXi version 8 VMware ESXi version 7 VMware vCenter Server version 8 VMware vCenter Server version 7 VMware Cloud Foundation version 4.x VMware Cloud Foundation version 5.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/24505

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.