Advisory Alert

Alert Number: **AAA20240704** **Date:** **July 4, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
IBM	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**, **Low**	Multiple Vulnerabilities

Description

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities in third-party components running on their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell Storage Monitoring and Reporting Vapp and Windows/Linux update Versions prior to 5.0.1.0 Dell Storage Resource Manager Vapp and Windows/Linux update Versions prior to 5.0.1.0 Dell NetWorker vProxy OVA Versions prior to 19.8.0.4 Dell NetWorker vProxy OVA Versions 19.9 through 19.9.0.7 Dell NetWorker vProxy OVA Versions 19.10 through 19.10.0.3
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000226624/dsa-2024-292-dell-storage-resource-manager-srm-and-dell-storage-monitoring-and-reporting-smr-security-update-for-multiple-third-party-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000226633/dsa-2024-022-security-update-for-dell-networker-vproxy-multiple-component-vulnerabilities

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2022-36765, CVE-2023-20569, CVE-2023-20577)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2022-36765** - A potential security vulnerability has been identified in HPE Compute Scale-up Server 3200, Superdome Flex and Superdome Flex 280 server platform firmware. These vulnerabilities could be exploited to allow local buffer overflow. **CVE-2023-20569** - A potential security vulnerability has been identified in certain HPE Cray Servers and HPE ProLiant DL/XL Servers using certain AMD EPYC processors. The vulnerability could be locally exploited to allow disclosure of information. **CVE-2023-20577** - A potential security vulnerability has been identified in certain HPE Cray Servers using certain AMD EPYC processors. The vulnerability could be locally exploited to allow arbitrary code execution vulnerability. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Compute Scale-up Server 3200 - Prior to v1.20.128 HPE Superdome Flex 280 Server - Prior to v1.80.20 HPE Superdome Flex Server - Prior to v3.100.26 HPE Cray EX235n Server - Prior to BIOS 1.3.1 (HFP 23.9) HPE Cray EX425 Compute Blade - Prior to BIOS 1.7.2 (HFP 23.9) HPE ProLiant DL325 Gen10 Plus server - Prior to BIOS 2.80 (HFP 23.8) HPE ProLiant DL385 Gen10 Plus server - Prior to BIOS 2.80 (HFP 23.8) HPE ProLiant XL645d Gen10 Plus Server - Prior to BIOS 2.80 (HFP 23.8) HPE ProLiant XL675d Gen10 Plus Server - Prior to BIOS 2.80 (HFP 23.8) HPE Cray EX235a Accelerator Blade - Prior to BIOS 1.8.0 (HFP 24.3.1) HPE Cray EX4252 Compute Blade - Prior to BIOS 1.5.0 (HFP 23.12) HPE Cray EX235a Accelerator Blade prior to BIOS 1.8.0 in HFP 24.3.1 HPE Cray EX235n Server prior to BIOS 1.3.1 in HFP 23.9 HPE Cray EX425 Compute Blade prior to BIOS 1.7.2 in HFP 23.9 HPE Cray EX4252 Compute Blade pior to BIOS 1.4.0 in HFP 23.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04632en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04545en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbcr04666en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-27351, CVE-2024-34064, CVE-2024-32879, CVE-2024-24786, CVE-2023-51775, CVE-2024-22353, CVE-2024-27270, CVE-2024-22354)
Description	IBM has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to XML External Entity Injections, Cross-site Scripting, Denial of Service, Security Restriction Bypass. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	IBM Storage Defender - Resiliency Service all versions IBM PowerVM Novalink 2.2.1, 2.2.0, 2.1.1, 2.1.0, 2.0.3.1, 2.0.3, 2.0.2.1, 2.0.2, 2.0.1 and 2.0.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7159632 • https://www.ibm.com/support/pages/node/7159508 • https://www.ibm.com/support/pages/node/7159505 • https://www.ibm.com/support/pages/node/7159506 • https://www.ibm.com/support/pages/node/7159507

Affected Product	**Ubuntu**
Severity	**High**, **Medium**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-26924, CVE-2024-26643, CVE-2024-21823, CVE-2024-26925, CVE-2024-26809, CVE-2024-2201, CVE-2021-33631, CVE-2024-26898, CVE-2021-47063, CVE-2024-24861, CVE-2023-52615, CVE-2024-26736, CVE-2024-26720, CVE-2024-23307, CVE-2024-26922, CVE-2023-6270, CVE-2024-26642)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause Denial of service and Sensitive information disclosure. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 23.10 Ubuntu 22.04 Ubuntu 20.04 Ubuntu 18.04 Ubuntu 16.04 Ubuntu 14.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://ubuntu.com/security/notices/USN-6863-1 • https://ubuntu.com/security/notices/USN-6873-1 • https://ubuntu.com/security/notices/USN-6872-1 • https://ubuntu.com/security/notices/USN-6869-1 • https://ubuntu.com/security/notices/USN-6868-1 • https://ubuntu.com/security/notices/USN-6866-1 • https://ubuntu.com/security/notices/USN-6865-1

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.