Advisory Alert

Alert Number: AAA20241022 **Date:** October 22, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Broadcom VMware	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Cleartext Storage of Sensitive Information Vulnerability
HPE	**High, Medium**	Multiple Vulnerabilities
IBM	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Broadcom VMware**
Severity	**Critical -** Initial release date **18th September 2024 (AAA20240918)**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-38812, CVE-2024-38813)
Description	Broadcom has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-38812 -** The vCenter Server contains a heap-overflow vulnerability in the implementation of the DCERPC protocol. A malicious actor with network access to vCenter Server may trigger this vulnerability by sending a specially crafted network packet potentially leading to remote code execution. **CVE-2024-38813** - The vCenter Server contains a privilege escalation vulnerability. A malicious actor with network access to vCenter Server may trigger this vulnerability to escalate privileges to root by sending a specially crafted network packet. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	VMware vCenter Server Version 8.0, 7.0 VMware Cloud Foundation 5.x , 5.1.x, 4.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/security-advisories/0/24968

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Cleartext Storage of Sensitive Information Vulnerability (CVE-2024-47244)
Description	Dell has released security updates addressing a Cleartext Storage of Sensitive Information Vulnerability that exists in their products. **CVE-2024-47244-** Dell PowerFlex Manager versions prior to 3.8.8 for RCM train 3.6.x, and versions prior to 4.6.0.1 for RCM trains 3.7.x and 3.8.x, contain a Cleartext Storage of Sensitive Information vulnerability. A low privileged attacker with adjacent network access could potentially exploit this vulnerability, leading to Information exposure and Elevation of privileges. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell PowerFlex rack running on PowerFlex Manager Versions prior to 4.6.0.1 Dell PowerFlex appliance running PowerFlex Manager Versions prior to 4.6.0.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000238943/dsa-2024-413-security-update-for-a-dell-powerflex-manager-multiple-vulnerabilities

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-24853, CVE-2024-25939, CVE-2024-23984, CVE-2024-21781, CVE-2024-21829)
Description	HPE has released security updates addressing Multiple Vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Privilege Escalation, Denial Of Service, and Information Disclosure. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Superdome Flex 280 Server - Prior to v1.90.12 HPE Superdome Flex Server - Prior to v4.0.10
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04714en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04718en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04717en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbhf04715en_us&docLocale=en_US

Affected Product	**IBM**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-45085, CVE-2024-45072)
Description	IBM has released security updates addressing Multiple Vulnerabilities that exist in IBM WebSphere Application Server. **CVE-2024-45085 -** IBM WebSphere Application Server is vulnerable to a denial of service, under certain configurations, caused by an unexpected specially crafted request. A remote attacker could exploit this vulnerability to cause an error resulting in a denial of service. **CVE-2024-45072**- IBM WebSphere Application Server is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A privileged user could exploit this vulnerability to expose sensitive information or consume memory resources. IBM advises to apply security fixes at your earliest to protect systems from potential threats.
sAffected Products	IBM WebSphere Remote Server Versions 9.1, 9.0, 8.5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.ibm.com/support/pages/node/7173599 • https://www.ibm.com/support/pages/node/7173600

Disclaimer

The information provided are gathered from official service provider's websites and portals. FinCSIRT strongly recommends members to apply security fixes as per the given guidelines, following the organization's patch and change management procedures to protect systems from potential threats.