Advisory Alert

Alert Number: AAA20240930 **Date:** September 30, 2024

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Remote Code Execution Vulnerability (RegreSSHion)
Dell	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
Commvault	**Medium**	DLL Injection Vulnerability

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Remote Code Execution Vulnerability (RegreSSHion) (CVE-2024-6387)
Description	HPE has released security updates addressing a potential security vulnerability, OpenSSH regreSSHion, which was discovered in HPE Superdome Flex and Flex 280 platforms. This vulnerability could be exploited to allow remote unauthenticated code execution. 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=hpesbhf04703en_us&docLocale=en_US

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities in third-party components, which in turn affect the Dell EMC VxRail 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 EMC VxRail Appliance 7.0.x versions prior to 7.0.531
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000229412/dsa-2024-392-security-update-for-dell-vxrail-7-0-531-multiple-third-party-component-vulnerabilities

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited to cause memory leakage, use-after-free conditions, null pointer dereference, SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Basesystem Module 15-SP5 Development Tools Module 15-SP5 Legacy Module 15-SP5 openSUSE Leap 15.5 , 15.6 openSUSE Leap Micro 5.5 SUSE Linux Enterprise Desktop 15 SP5 Multiple SUSE Linux Enterprise High Availability Extension 15 SP5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5, 15-SP6 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5, SP6 SUSE Linux Enterprise Server 11 SP4, 11 SP4 LTSS EXTREME CORE 11-SP4 SUSE Linux Enterprise Server 15 SP5, SP6 SUSE Linux Enterprise Server for SAP Applications 15 SP5, 15 SP6 SUSE Linux Enterprise Workstation Extension 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.suse.com/support/update/announcement/2024/suse-su-20243468-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243467-1/ • https://www.suse.com/support/update/announcement/2024/suse-su-20243483-1/

Affected Product	**Commvault**
Severity	**Medium**
Affected Vulnerability	DLL Injection Vulnerability
Description	Commvault has released security updates addressing a DLL injection vulnerability when installing maintenance releases for Commvault products on Windows. Commvault advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Commvault 11.36.0 running on Windows Commvault 11.34.0 running on Windows Commvault 11.32.0 running on Windows Commvault 11.28.0 running on Windows Commvault 11.20.0 running on Windows
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://documentation.commvault.com/securityadvisories/CV_2024_09_2.html

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.