Advisory Alert

Alert Number: **AAA20241204** **Date:** **December 4, 2024**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
Veeam	**Critical**	Remote Code Execution Vulnerability
Dell	**Critical**	Multiple Vulnerabilities
Veeam	**High**	Multiple Vulnerabilities
Dell	**High**	Multiple Vulnerabilities
HPE	**High**	Multiple Vulnerabilities
Juniper	**High**	Improper Handling of Exceptional Conditions Vulnerability
SUSE	**High**	Multiple Vulnerabilities
F5	**High**	Multiple Vulnerabilities
Red Hat	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**Veeam**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2024-42448)
Description	Veeam has released security updates addressing a Remote Code Execution vulnerability that exists in their products. The vulnerability exists in the the VSPC management agent machine, under the condition that the management agent is authorized on the server. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Service Provider Console 8.1.0.21377 and all earlier versions of 8 and 7 builds.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.veeam.com/kb4679

Affected Product	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2017-16931, CVE-2017-7376, CVE-2016-4658, CVE-2015-8710, CVE-2016-4448, CVE-2017-7375, CVE-2021-3518, CVE-2016-5131, CVE-2017-15412, CVE-2017-5130, CVE-2021-3517, CVE-2016-1762, CVE-2016-1840, CVE-2022-40304, CVE-2016-1834, CVE-2015-6838, CVE-2019-19956, CVE-2017-16932, CVE-2022-40303, CVE-2016-3627, CVE-2013-1969, CVE-2022-23308, CVE-2016-4447, CVE-2015-6837, CVE-2024-25062, CVE-2016-4483, CVE-2018-14404, CVE-2015-8806, CVE-2015-5312, CVE-2016-4449, CVE-2013-0339, CVE-2012-5134, CVE-2012-2871, CVE-2016-9596, CVE-2023-28484, CVE-2023-45322, CVE-2023-29469, CVE-2022-29824, CVE-2016-2073, CVE-2017-18258, CVE-2021-3541, CVE-2016-9598, CVE-2015-8241, CVE-2021-3537, CVE-2015-8242, CVE-2016-1837, CVE-2016-1838, CVE-2016-9318, CVE-2016-1833, CVE-2016-1836, CVE-2016-1839, CVE-2015-7500, CVE-2015-8317, CVE-2013-2877, CVE-2015-7497, CVE-2015-7499, CVE-2014-3660, CVE-2015-7498, CVE-2013-0338)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities that 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 NetWorker Server Versions 19.11 through 19.11.0.1 Dell NetWorker Server Versions 19.10 through 19.10.0.5 Dell NetWorker Server Versions 19.9 through 19.9.0.7 Dell NetWorker Server Versions prior to 19.8
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000255975/dsa-2024-451-security-update-for-dell-networker-for-libxml2-2-9-0-vulnerabilities

Affected Product	**Veeam**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40717, CVE-2024-42451, CVE-2024-42452, CVE-2024-42453, CVE-2024-42455, CVE-2024-42456, CVE-2024-42457, CVE-2024-45204, CVE-2024-42449)
Description	Veeam has released security updates addressing multiple vulnerabilities that exist in their products. Exploitation of these vulnerabilities may lead to privilege escalation, file deletion, credential extraction. Veeam advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Veeam Service Provider Console 8.1.0.21377 and all earlier versions of 8 and 7 builds. Veeam Backup & Replication 12.2.0.334 and all earlier version 12 builds. Veeam Agent for Microsoft Windows 6.0, 6.1, 6.2
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.veeam.com/kb4693 • https://www.veeam.com/kb4679

Affected Product	**Dell**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-42950, CVE-2024-25062, CVE-2024-21235, CVE-2024-21210, CVE-2024-21208, CVE-2024-21217, CVE-2024-47476, CVE-2024-42422)
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities that 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 NetWorker Runtime Environment Version NRE 8.0.22 Dell NetWorker Management Console Version NRE 8.0.22 Dell NetWorker Client Versions 19.11 through 19.11.0.2 Dell NetWorker Client Versions prior to 19.10.0.6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000255884/dsa-2024-477-security-update-for-dell-networker-runtime-environment-nre-multiple-component-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000255892/dsa-2024-478-security-update-for-dell-networker-vulnerabilities

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-51771, CVE-2024-51772, CVE-2024-51773, CVE-2024-53672)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-51771 -** A vulnerability in the HPE Aruba Networking ClearPass Policy Manager web-based management interface could allow an authenticated remote threat actor to conduct a remote code execution attack. Successful exploitation could enable the attacker to run arbitrary commands on the underlying operating system. **CVE-2024-51772 -** An authenticated RCE vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploitation could allow an attacker to execute arbitrary commands on the underlying operating system. **CVE-2024-51773 -** A vulnerability in the HPE Aruba Networking ClearPass Policy Manager web-based management interface could allow an authenticated remote Attacker to conduct a stored cross-site scripting (XSS) attack. Successful exploitation could enable a threat actor to perform any actions the user is authorized to do, including accessing the user's data and altering information within the user's permissions. This could lead to data modification, deletion, or theft, including unauthorized access to files, file deletion, or the theft of session cookies, which an attacker could use to hijack a user's session. **CVE-2024-53672 -** A vulnerability in the ClearPass Policy Manager web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. Successful exploit could allow an attacker to execute arbitrary commands as a lower privileged user on the underlying operating system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking ClearPass Policy Manager 6.12.x: 6.12.2 and below HPE Aruba Networking ClearPass Policy Manager 6.11.x: 6.11.9 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04761en_us&docLocale=en_US

Affected Product	**Juniper**
Severity	**High**
Affected Vulnerability	Improper Handling of Exceptional Conditions Vulnerability (CVE-2024-30382)
Description	Juniper has issued security updates addressing an Improper Handling of Exceptional Conditions vulnerability that exists in their products. The vulnerability exists in the routing protocol daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows a network-based, unauthenticated attacker to send a specific routing update, causing an rpd core due to memory corruption, leading to a Denial of Service (DoS). Juniper advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Junos OS: • all versions before 20.4R3-S10, • from 21.2 before 21.2R3-S8, • from 21.3 before 21.3R3, • from 21.4 before 21.4R3, • from 22.1 before 22.1R2; Junos OS Evolved: • all versions before 21.2R3-S8-EVO • from 21.3 before 21.3R3-EVO • from 21.4 before 21.4R3-EVO • from 22.1 before 22.1R2-EVO
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://supportportal.juniper.net/s/article/2024-04-Security-Bulletin-Junos-OS-and-Junos-OS-Evolved-Junos-OS-and-Junos-OS-Evolved-RPD-crash-when-CoS-based-forwarding-CBF-policy-is-configured-CVE-2024-30382?language=en_US

Affected Product	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2021-47517, CVE-2024-43861)
Description	SUSE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Memory leakage and Use-after-free conditions SUSE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	openSUSE Leap 15.5 SUSE Linux Enterprise High Performance Computing 15 SP5 SUSE Linux Enterprise Live Patching 15-SP5 SUSE Linux Enterprise Micro 5.5 SUSE Linux Enterprise Real Time 15 SP5 SUSE Linux Enterprise Server 15 SP5 SUSE Linux Enterprise Server for SAP Applications 15 SP5
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2024/suse-su-20244160-1/

Affected Product	**F5**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-41090, CVE-2024-41091)
Description	F5 has issued security updates addressing multiple vulnerabilities that exist in their products. **CVE-2024-41090** - In the Linux kernel, the following vulnerability has been resolved: tap: add missing verification for short frame The cited commit missed to check against the validity of the frame length in the tap_get_user_xdp() path, which could cause a corrupted skb to be sent downstack. Even before the skb is transmitted, the tap_get_user_xdp()-->skb_set_network_header() may assume the size is more than ETH_HLEN. Once transmitted, this could either cause out-of-bound access beyond the actual length, or confuse the underlayer with incorrect or inconsistent header length in the skb metadata. In the alternative path, tap_get_user() already prohibits short frame which has the length less than Ethernet header size from being transmitted. This is to drop any frame shorter than the Ethernet header size just like how tap_get_user() does. **CVE-2024-41091** - In the Linux kernel, the following vulnerability has been resolved: tun: add missing verification for short frame The cited commit missed to check against the validity of the frame length in the tun_xdp_one() path, which could cause a corrupted skb to be sent downstack. Even before the skb is transmitted, the tun_xdp_one-->eth_type_trans() may access the Ethernet header although it can be less than ETH_HLEN. Once transmitted, this could either cause out-of-bound access beyond the actual length, or confuse the underlayer with incorrect or inconsistent header length in the skb metadata. In the alternative path, tun_get_user() already prohibits short frame which has the length less than Ethernet header size from being transmitted for IFF_TAP. This is to drop any frame shorter than the Ethernet header size just like how tun_get_user() does. F5 advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	BIG-IP Next (all modules) 20.2.1 BIG-IP Next Central Manager 20.2.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://my.f5.com/manage/s/article/K000148830

Affected Product	**Red Hat**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2023-0597,CVE-2023-52619,CVE-2023-52749,CVE-2023-52881,CVE-2024-26984,CVE-2024-27399,CVE-2024-36920,CVE-2024-37356,CVE-2024-40988,CVE-2024-41009,CVE-2024-41014,CVE-2024-41041,CVE-2024-41093,CVE-2024-42154,CVE-2024-42240,CVE-2024-43854,CVE-2022-48804,CVE-2023-52635,CVE-2023-52775,CVE-2023-52811,CVE-2024-26601,CVE-2024-26615,CVE-2024-26686,CVE-2024-26704,CVE-2024-36960,CVE-2024-38384,CVE-2024-38541,CVE-2024-38555,CVE-2024-39507,CVE-2024-40997,CVE-2024-41007,CVE-2024-41008,CVE-2024-41031,CVE-2024-41038,CVE-2024-41056,CVE-2024-42228,CVE-2024-42237,CVE-2024-42238,CVE-2024-42241,CVE-2024-42243,CVE-2024-42244,CVE-2024-42271,CVE-2024-44989)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause information leakage, race conditions, system crash. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.2 s390x Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 9.4 s390x Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.2 x86_64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 9.4 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.2 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 9.4 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 9.4 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.2 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 9.4 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.2 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 9.4 ppc64le Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for NFV for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.2 x86_64 Red Hat Enterprise Linux for Real Time for x86_64 - 4 years of updates 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 9.4 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.2 x86_64 Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 9.4 x86_64 Red Hat Enterprise Linux Server - AUS 9.2 x86_64 Red Hat Enterprise Linux Server - AUS 9.4 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.2 ppc64le Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 9.4 ppc64le
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2024:10773 • https://access.redhat.com/errata/RHSA-2024:10772 • https://access.redhat.com/errata/RHSA-2024:10771

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.