Advisory Alert

Alert Number: **AAA20250108** **Date:** **January 8, 2025**

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
HPE	**High**	Multiple Command Injection Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Qnap	**High, Medium**	Multiple Vulnerabilities
SonicWall	**High, Medium**	Multiple Vulnerabilities
Ubuntu	**High, Medium**	Multiple Vulnerabilities
Dell	**Medium**	Uncontrolled Resource Consumption Vulnerability

Description

Affected Product	**HPE**
Severity	**High**
Affected Vulnerability	Multiple Command Injection Vulnerabilities (CVE-2024-54006, CVE-2024-54007)
Description	HPE has released security updates addressing multiple Command Injection vulnerabilities that exist in HPE Aruba Networking 501 Wireless Client Bridge. Successful exploitation of these vulnerabilities result in the ability of an attacker to execute arbitrary commands as a privileged user on the underlying operating system. Exploitation requires administrative authentication credentials on the host system. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking 501 Wireless Client Bridge versions 2.1.1.0-B0030 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04763en_us&docLocale=en_US

Affected Product	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53122, CVE-2024-53088, CVE-2024-26830, CVE-2024-41040, CVE-2024-35890, CVE-2024-46713, CVE-2024-50208, CVE-2024-50252, CVE-2024-38598)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. Successful exploitation of these vulnerabilities results in data corruption, data leak, Denial of Service conditions. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:0067 • https://access.redhat.com/errata/RHSA-2025:0066 • https://access.redhat.com/errata/RHSA-2025:0065 • https://access.redhat.com/errata/RHSA-2025:0064 • https://access.redhat.com/errata/RHSA-2025:0063 • https://access.redhat.com/errata/RHSA-2025:0062 • https://access.redhat.com/errata/RHSA-2025:0061 • https://access.redhat.com/errata/RHSA-2025:0060 • https://access.redhat.com/errata/RHSA-2025:0059 • https://access.redhat.com/errata/RHSA-2025:0058 • https://access.redhat.com/errata/RHSA-2025:0057 • https://access.redhat.com/errata/RHSA-2025:0056 • https://access.redhat.com/errata/RHSA-2025:0055 • https://access.redhat.com/errata/RHSA-2025:0054 • https://access.redhat.com/errata/RHSA-2025:0053 • https://access.redhat.com/errata/RHSA-2025:0052 • https://access.redhat.com/errata/RHSA-2025:0051 • https://access.redhat.com/errata/RHSA-2025:0050 • https://access.redhat.com/errata/RHSA-2025:0049

Affected Product	**Qnap**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-48859, CVE-2024-48865, CVE-2024-48866, CVE-2024-48867, CVE-2024-48868, CVE-2024-50393, CVE-2024-50402, CVE-2024-50403, CVE-2024-50404)
Description	Qnap has released security updates addressing multiple vulnerabilities that exist in QTS, QuTS hero and Qsync Central. These vulnerabilities could be exploited by malicious users to cause Remote Command Injection, Data Modification, Information Disclosure, Privilege Escalation, Path Traversal. Qnap advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	QTS 5.1.x versions prior to 5.1.9.2954 build 20241120 QTS 5.2.x versions prior to 5.2.2.2950 build 20241114 QuTS hero h5.1.x versions prior to h5.1.9.2954 build 20241120 QuTS hero h5.2.x versions prior to h5.2.2.2952 build 20241116 Qsync Central 4.4.x versions prior to 4.4.0.16_20240819
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.qnap.com/en/security-advisory/qsa-24-49 • https://www.qnap.com/en/security-advisory/qsa-24-48

Affected Product	**SonicWall**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-40762, CVE-2024-53704, CVE-2024-53705, CVE-2024-53706, CVE-2024-12802, CVE-2024-12803, CVE-2024-12805, CVE-2024-12806)
Description	SonicWall has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause Authentication Bypass, Server-Side Request Forgery, Local Privilege Escalation, Remote Code Execution, System Crash. SonicWall advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• Versions prior to 6.5.4.15-117n of Gen6 Hardware Firewalls: SOHOW, TZ 300, TZ 300W, TZ 400, TZ 400W, TZ 500, TZ 500W, TZ 600, NSA 2650, NSA 3600, NSA 3650, NSA 4600, NSA 4650, NSA 5600, NSA 5650, NSA 6600, NSA 6650, SM 9200, SM 9250, SM 9400, SM 9450, SM 9600, SM 9650, TZ 300P, TZ 600P, SOHO 250, SOHO 250W, TZ 350, TZ 350W • Versions prior to 6.5.4.4-44v-21-2472 of Gen6 NSv: NSv10, NSv25, NSv50, NSv100, NSv200, NSv300, NSv400, NSv800, NSv1600 • Versions prior to 7.1.3-7015 of Gen7 NSv: NSv 270, NSv 470, NSv 870 • Versions prior to 7.1.3-7015 of Gen7 Firewalls: TZ270, TZ270W, TZ370, TZ370W, TZ470, TZ470W, TZ570, TZ570W, TZ570P, TZ670, NSa 2700, NSa 3700,NSa 4700, NSa 5700, NSa 6700, NSsp 10700, NSsp 11700, NSsp 13700, NSsp 15700 • TZ80 Versions 8.0.0-8035
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0003 • https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0001 • https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2025-0004

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2024-53057, CVE-2024-50264, CVE-2024-49967)
Description	Ubuntu has released security updates addressing multiple vulnerabilities that exist in Ubuntu Linux kernel. **CVE-2024-53057** - net/sched: stop qdisc_tree_reduce_backlog on TC_H_ROOT In qdisc_tree_reduce_backlog, Qdiscs with major handle ffff: are assumed to be either root or ingress. This assumption is bogus since it's valid to create egress qdiscs with major handle ffff: Budimir Markovic found that for qdiscs like DRR that maintain an active class list, it will cause a UAF with a dangling class pointer. In 066a3b5b2346, the concern was to avoid iterating over the ingress qdisc since its parent is itself. The proper fix is to stop when parent TC_H_ROOT is reached because the only way to retrieve ingress is when a hierarchy which does not contain a ffff: major handle call into qdisc_lookup with TC_H_MAJ(TC_H_ROOT). In the scenario where major ffff: is an egress qdisc in any of the tree levels, the updates will also propagate to TC_H_ROOT, which then the iteration must stop. net/sched/sch_api.c | 2 +- 1 file changed, 1 insertion(+), 1 deletion(-) **CVE-2024-50264** - vsock/virtio: Initialization of the dangling pointer occurring in vsk->trans During loopback communication, a dangling pointer can be created in vsk->trans, potentially leading to a Use-After-Free condition. This issue is resolved by initializing vsk->trans to NULL. **CVE-2024-49967** - ext4: no need to continue when the number of entries is 1 Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 24.04 Ubuntu 22.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7167-2

Affected Product	**Dell**
Severity	**Medium**
Affected Vulnerability	Uncontrolled Resource Consumption Vulnerability (CVE-2024-47239)
Description	Dell has released security updates addressing Uncontrolled Resource Consumption Vulnerability that exists in PowerScale OneFS. **CVE-2024-47239** - Dell PowerScale OneFS versions 8.2.2.x through 9.9.0.0 contain an uncontrolled resource consumption vulnerability. A remote low privileged attacker could potentially exploit this vulnerability, leading to denial of service. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	PowerScale OneFS Version 8.2.2.x through 9.9.0.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000269590/dsa-2024-480-security-update-for-dell-powerscale-onefs-security-vulnerability

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.