Advisory Alert

Alert Number: AAA20260722 **Date:** July 22, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
HPE	**Critical**	Security Update
Dell	**Critical**	Multiple Vulnerabilities
Oracle	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
SUSE	**High**	Multiple Vulnerabilities
HPE	**High**, Low	Multiple Vulnerabilities

Description

Vendor	**HPE**
Severity	**Critical**
Affected Vulnerability	Security Update (CVE-2026-48020)
Description	HPE has released a security update addressing a vulnerability that exists in their products. **CVE-2026-48020:** Traefik is an HTTP reverse proxy and load balancer. Prior to 2.11.48, 3.6.19, and 3.7.3, there is a high severity vulnerability in Traefik's StripPrefix middleware that allows an unauthenticated attacker to bypass route-level authentication and authorization. When a public router matches on a PathPrefix rule and applies the StripPrefix middleware, a request path containing .. or its percent-encoded form %2e%2e can match the public route at routing time and then, after the prefix is stripped and the path is normalized, resolve to a path served by a separate, authenticated router. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking Private 5G Core versions prior to 1.26.1.1.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05083en_us&docLocale=en_US

Vendor	**Dell**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Dell has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Dell advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Dell Networking OS10 Versions prior to 10.6.0.9 PowerEdge: • ConnectX-5 Versions prior to 16.35.80.02 • ConnectX-6 LX Versions prior to 26.46.30.48 • ConnectX-6 DX Versions prior to 22.46.30.48 • ConnectX-7 NDR Versions prior to 28.46.30.48 • ConnectX-8 XDR Versions prior to 40.46.3048
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000491127/dsa-2026-299-security-update-for-dell-networking-os10-vulnerabilities • https://www.dell.com/support/kbdoc/en-us/000491103/dsa-2026-323-security-update-for-nvidia-networking-bluefield-and-connectx-vulnerabilities

Vendor	**Oracle**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities
Description	Oracle has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Oracle advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Multiple Products
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.oracle.com/security-alerts/cpujul2026.html https://www.oracle.com/security-alerts/bulletinjul2026.html

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-71113, CVE-2025-71147, CVE-2026-23168, CVE-2026-31530, CVE-2026-46116, CVE-2026-46150, CVE-2026-46215, CVE-2026-52976, CVE-2026-52950, CVE-2026-53009, CVE-2026-53071, CVE-2026-46117)
Description	Red Hat has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. Red Hat advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for x86_64 10 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 10 ppc64le Red Hat CodeReady Linux Builder for ARM 64 10 aarch64 Red Hat CodeReady Linux Builder for IBM z Systems 10 s390x Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.2 x86_64 Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.2 s390x Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support 10.2 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.2 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.2 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.2 aarch64 Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.2 x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.2 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.2 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.2 ppc64le Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 10.2 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 10.2 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 10.2 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 10.2 s390x Red Hat Enterprise Linux for x86_64 8 x86_64 Red Hat Enterprise Linux for IBM z Systems 8 s390x Red Hat Enterprise Linux for Power, little endian 8 ppc64le Red Hat Enterprise Linux for ARM 64 8 aarch64 Red Hat CodeReady Linux Builder for x86_64 8 x86_64 Red Hat CodeReady Linux Builder for Power, little endian 8 ppc64le Red Hat CodeReady Linux Builder for ARM 64 8 aarch64 Red Hat Enterprise Linux for x86_64 - Extended Life Cycle 8.10 x86_64 Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle 8.10 aarch64 Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle 8.10 ppc64le Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle 8.10 s390x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:42919 https://access.redhat.com/errata/RHSA-2026:42552

Vendor	**SUSE**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-43109, CVE-2026-46052, CVE-2026-46071, CVE-2026-46076, CVE-2026-46116, CVE-2026-46173, CVE-2026-46229, CVE-2026-46242, CVE-2026-46253, CVE-2026-46266, CVE-2026-46274, CVE-2026-46289, CVE-2026-46319, CVE-2026-46320, CVE-2026-46330, CVE-2026-46331, CVE-2026-52909, CVE-2026-52918, CVE-2026-52923, CVE-2026-52924, CVE-2026-52933, CVE-2026-52943, CVE-2026-52955, CVE-2026-52956, CVE-2026-52958, CVE-2026-52969, CVE-2026-52972, CVE-2026-52993, CVE-2026-53016, CVE-2026-53041, CVE-2026-53052, CVE-2026-53053, CVE-2026-53071, CVE-2026-53072, CVE-2026-53133, CVE-2026-53178, CVE-2026-53182, CVE-2026-53196, CVE-2026-53253, CVE-2026-53256, CVE-2026-53357, CVE-2026-53359, CVE-2026-53362, CVE-2026-53366)
Description	SUSE has released a security update addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. SUSE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	openSUSE Leap 15.6 SUSE Linux Enterprise High Availability Extension 15 SP6 SUSE Linux Enterprise Live Patching 15-SP6 SUSE Linux Enterprise Real Time 15 SP6 SUSE Linux Enterprise Server 15 SP6 SUSE Linux Enterprise Server 15 SP6 LTSS SUSE Linux Enterprise Server for SAP Applications 15 SP6
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.suse.com/support/update/announcement/2026/suse-su-20263156-1/

Vendor	**HPE**
Severity	**High**, **Low**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-44880, CVE-2026-63453, CVE-2026-63454, CVE-2026-35387, CVE-2026-44878, CVE-2026-44879)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise the affected systems. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	AOS-CX 10.13.xxxx: 10.13.1170 and below AOS-CX 10.16.xxxx: 10.16.1040 and below AOS-CX 10.17.xxxx: 10.17.1010 and below ECOS 9.4.x.x: 9.4.6.x and below ECOS 9.5.x.x: 9.5.6.x and below ECOS 9.6.x.x: 9.6.1.x and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05081en_us&docLocale=en_US • https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05013en_us&docLocale=en_US

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.