Advisory Alert

Alert Number: AAA20261028 **Date:** October 28, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Red Hat	**Critical**	Multiple Vulnerabilities
WatchGuard	**Critical**	Multiple Vulnerabilities
Broadcom	**Critical**	Remote Code Execution Vulnerability
Red Hat	**High**	Multiple Vulnerabilities
WatchGuard	**High**	Multiple Vulnerabilities

Description

Vendor	**Red Hat**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-35973, CVE-2026-0799, CVE-2026-5260, CVE-2026-6893, CVE-2026-8924, CVE-2026-10723, CVE-2026-15816, CVE-2026-16445, CVE-2026-19666, CVE-2026-19667, CVE-2026-19953, CVE-2026-34182, CVE-2026-34183, CVE-2026-40467, CVE-2026-40468, CVE-2026-42011, CVE-2026-42012, CVE-2026-42013, CVE-2026-43114, CVE-2026-45445, CVE-2026-45447, CVE-2026-54369, CVE-2026-58014, CVE-2026-59995, CVE-2026-59999, CVE-2026-60002, CVE-2026-63382, CVE-2026-63383, CVE-2026-63384, CVE-2026-63385, CVE-2026-63387, CVE-2026-63388, CVE-2026-64564, CVE-2026-66046, CVE-2026-68108, CVE-2026-68121, CVE-2026-68123, CVE-2026-68257, CVE-2026-80274, CVE-2026-80792, CVE-2026-80863, CVE-2026-80864, CVE-2026-80887, CVE-2026-80921, CVE-2026-81003, CVE-2026-86138, CVE-2026-86140, CVE-2026-86142, CVE-2026-86143, CVE-2026-86144, CVE-2026-86145, CVE-2026-89161, CVE-2026-89480, CVE-2026-89481, CVE-2026-89663, CVE-2026-89669, CVE-2026-89690, CVE-2026-89811, CVE-2026-89894, CVE-2026-89972, CVE-2026-90036, CVE-2026-90227, CVE-2026-93207, CVE-2026-93228, CVE-2026-93288, CVE-2026-93817, CVE-2026-93990, CVE-2026-94640, CVE-2026-97417, CVE-2026-99999, CVE-2026-103111, CVE-2026-103262, CVE-2026-114406)
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 OpenShift Container Platform 4.22 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat OpenShift Container Platform 4.21 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat OpenShift Container Platform 4.20 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat OpenShift Container Platform 4.19 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat OpenShift Container Platform 4.18 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat OpenShift Container Platform 4.16 (RHEL 9): aarch64, ppc64le, s390x, x86_64 Red Hat OpenShift Container Platform 4.14 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 Red Hat OpenShift Container Platform 4.12 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:89333 • https://access.redhat.com/errata/RHSA-2026:89651 • https://access.redhat.com/errata/RHSA-2026:89232 • https://access.redhat.com/errata/RHSA-2026:89725 • https://access.redhat.com/errata/RHSA-2026:90272 • https://access.redhat.com/errata/RHSA-2026:89714 • https://access.redhat.com/errata/RHSA-2026:89838 • https://access.redhat.com/errata/RHSA-2026:89197

Vendor	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-93866, CVE-2026-93857, CVE-2026-103593, CVE-2026-93865, CVE-2026-103594, CVE-2026-112709, CVE-2026-112710)
Description	WatchGuard 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. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Fireware OS: • Default >= 2025.1, < 2026.4, >= 12.0, < 12.12.4 • T15/T35 >= 12.0, < 12.5.22
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.watchguard.com/CVE-2026-93866/ • https://psirt.watchguard.com/CVE-2026-93857/ • https://psirt.watchguard.com/CVE-2026-103593/ • https://psirt.watchguard.com/CVE-2026-93865/ • https://psirt.watchguard.com/CVE-2026-103594/ • https://psirt.watchguard.com/CVE-2026-112709/ • https://psirt.watchguard.com/CVE-2026-112710/

Vendor	**Broadcom**
Severity	**Critical**
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-111497)
Description	Broadcom has released a security update addressing a vulnerability that exists in their products. **CVE-2026-111497:** A buffer overflow vulnerability in the Brotli decoder (c/dec/decode.c) in Google Brotli versions 1.0.3 through 1.2.0 on all platforms allows a remote unauthenticated attacker to corrupt adjacent decoder state memory, disclose sensitive memory contents, cause a denial of service, or potentially execute arbitrary code using a crafted Brotli-compressed stream. Users need to update any Brotli libraries or binaries between 1.0.3 through 1.2.0 to the latest available version: 1.0.10 or 1.1.1 or 1.2.1. Broadcom advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• VMware Cloud Foundation, VMware vSphere Foundation - Versions 9.1.1 • VMware Cloud Foundation, VMware vSphere Foundation - Versions 9.0.x, 9.1.0 • VMware Cloud Foundation - Versions 5.2.x
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.broadcom.com/web/ecx/support-content-notification/-/external/content/SecurityAdvisories/0/39445

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-33814, CVE-2026-46086, CVE-2026-52972, CVE-2026-53236, CVE-2026-53388, CVE-2026-62146, CVE-2026-63831, CVE-2026-63978, CVE-2026-63979, CVE-2026-64027, CVE-2026-64109, CVE-2026-64523, CVE-2026-68136, CVE-2026-68338, CVE-2026-72083, CVE-2026-72243, CVE-2026-74515, CVE-2026-74631, CVE-2026-80824, CVE-2026-89638, CVE-2026-89777, CVE-2026-89846, CVE-2026-93262, CVE-2026-99999, CVE-2026-111943)
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 OpenShift Container Platform 4.21 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 • Red Hat OpenShift Container Platform 4.16 (RHEL 8 / 9): aarch64, ppc64le, s390x, x86_64 • Red Hat Enterprise Linux Server 6: • Extended Life Cycle Support Extension: i386, s390x, x86_64 • Red Hat Enterprise Linux 8: • 8.6: Advanced Update Support (AUS) (x86_64), Extended Life Cycle Long Life (x86_64) • Red Hat Enterprise Linux 10: • Base & CRB 10: aarch64, ppc64le, s390x, x86_64 • Hidden Content 10: x86_64 • 10.2: Extended Update Support (EUS) & CRB EUS (all archs), 4 Years of Updates (aarch64, s390x, x86_64), 4 Years of Support (ppc64le), Extended Life Cycle (all archs)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:89713 • https://access.redhat.com/errata/RHSA-2026:90933 • https://access.redhat.com/errata/RHSA-2026:91493 • https://access.redhat.com/errata/RHSA-2026:91565 • https://access.redhat.com/errata/RHSA-2026:89229

Vendor	**WatchGuard**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-93864, CVE-2026-111107, CVE-2026-104381, CVE-2026-82332, CVE-2026-90442, CVE-2026-113881, CVE-2026-93434, CVE-2026-90464, CVE-2026-93862, CVE-2026-90465, CVE-2026-115495)
Description	WatchGuard 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. WatchGuard advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Fireware OS (Default) • >= 2025.1, < 2026.4 • >= 12.0, < 12.12.4 Fireware OS (T15/T35) • >= 12.0, < 12.5.22 Fireware OS (All platforms) • >= 12.0, < 12.5.22 Mobile VPN with SSL Client (Windows) • >= 12.0, < 2026.4
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.watchguard.com/CVE-2026-93864/ • https://psirt.watchguard.com/CVE-2026-111107/ • https://psirt.watchguard.com/CVE-2026-104381/ • https://psirt.watchguard.com/CVE-2026-82332/ • https://psirt.watchguard.com/CVE-2026-90442/ • https://psirt.watchguard.com/CVE-2026-113881/ • https://psirt.watchguard.com/CVE-2026-93434/ • https://psirt.watchguard.com/CVE-2026-90464/ • https://psirt.watchguard.com/CVE-2026-93862/ • https://psirt.watchguard.com/CVE-2026-90465/ • https://psirt.watchguard.com/CVE-2026-115495/

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.