



Advisory Alert

Alert Number: AAA20260930 Date: September 30, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
WatchGuard	Critical	Remote Code Execution Vulnerability
HPE	Critical	Multiple Vulnerabilities
Red Hat	High	Multiple Vulnerabilities
Dell	High	OS Command Injection Vulnerability
WatchGuard	High, Medium	Multiple Vulnerabilities
HPE	High, Medium, Low	Multiple Vulnerabilities
Ubuntu	High, Medium, Low	Multiple Vulnerabilities
OpenSSL	Low	Multiple Vulnerabilities

Description

Vendor	WatchGuard
Severity	Critical
Affected Vulnerability	Remote Code Execution Vulnerability (CVE-2026-86131)
Description	WatchGuard has released a security update addressing a vulnerability that exists in their products. CVE-2026-86131: A code injection vulnerability in WatchGuard Fireware OS's BOVPN Over TLS client configuration handling allows an attacker who controls the remote VPN server to execute arbitrary commands as root on the connecting Firebox. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS (Default): 2026.3 up to but not including 2026.3.2 2025.0 up to but not including 2026.2.3 12.0 up to but not including 12.12.3 Fireware OS (T15/T35): 12.0 up to but not including 12.5.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-86131/

Vendor	HPE
Severity	Critical
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76721, CVE-2026-76722, CVE-2026-76723, CVE-2026-76724, CVE-2026-76725)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Instant ON 3.4.1.0 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05150en_us&docLocale=en_US

Vendor	Red Hat
Severity	High
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-8458, CVE-2026-8927, CVE-2026-53266, CVE-2022-49670, CVE-2026-31581, CVE-2026-52924, CVE-2026-52993, CVE-2026-53002, CVE-2026-53059, CVE-2026-53071, CVE-2026-53091, CVE-2026-53185, CVE-2026-64191, CVE-2026-68294, CVE-2026-68480, CVE-2026-72098, CVE-2026-74746, CVE-2026-27727, CVE-2026-27830, CVE-2026-42578, CVE-2026-42581, CVE-2026-42583, CVE-2026-42584, CVE-2026-42585, CVE-2026-13221, CVE-2026-53784, CVE-2026-53785, CVE-2026-53789, CVE-2026-53790, CVE-2026-53791, CVE-2026-53793, CVE-2026-53795, CVE-2026-53802, CVE-2026-53803, CVE-2026-70452, CVE-2026-70453, CVE-2026-70454, CVE-2026-70456, CVE-2026-70457, CVE-2026-70458, CVE-2026-70460, CVE-2026-70461, CVE-2026-70463, CVE-2026-70464, CVE-2026-33814)
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 (General) - OpenShift Dev Spaces - JBoss EAP 7.3: Extended Update Support (EUS) (x86_64) OpenShift 4.22: - RHEL 9 Base: Standard (x86_64), Power (ppc64le), IBM Z & LinuxONE (s390x), ARM 64 (aarch64) - RHEL 8 Base: Standard (x86_64), Power (ppc64le), IBM Z & LinuxONE (s390x), ARM 64 (aarch64) RHEL 9.4: 4 Years of Updates: aarch64, s390x - Advanced Update Support (AUS): x86_64 - Extended Life Cycle (ELC): aarch64, ppc64le, s390x, x86_64 - Update Services for SAP Solutions (E4S): ppc64le, x86_64 Legacy / Extended Support: - RHEL 6: Extended Life Cycle Support Extension (ELS) (i386, s390x, x86_64)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://access.redhat.com/errata/RHSA-2026:73516 https://access.redhat.com/errata/RHSA-2026:73732 https://access.redhat.com/errata/RHSA-2026:73645 https://access.redhat.com/errata/RHSA-2026:73644 https://access.redhat.com/errata/RHSA-2026:71446 https://access.redhat.com/errata/RHSA-2026:73518

Vendor	Dell
Severity	High
Affected Vulnerability	OS Command Injection Vulnerability (CVE-2026-101207)
Description	Dell has released a security update addressing a vulnerability that exists in their products. CVE-2026-101207: Dell OpenManage Integration with Microsoft Windows Admin Center, versions prior to 3.7.0, contains an Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection') vulnerability. A low privileged attacker with remote access could potentially exploit this vulnerability, leading to Remote execution. Dell advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Dell OpenManage Integration with Microsoft Windows Admin Center (OMIMSWAC) versions prior to 3.7.0
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.dell.com/support/kbdoc/en-us/000515026/dsa-2026-442-security-update-for-dell-openmanage-integration-with-microsoft-windows-admin-center

Vendor	WatchGuard
Severity	High, Medium
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-86101, CVE-2026-13046, CVE-2026-18145, CVE-2026-86104, CVE-2026-18105, CVE-2026-86128, CVE-2026-81433, CVE-2026-86136, CVE-2026-90441, CVE-2026-86105, CVE-2026-86132, CVE-2026-13224, CVE-2026-86133)
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): 2026.3 up to but not including 2026.3.2 2025.0 up to but not including 2026.2.3 12.0 up to but not including 12.12.3 Fireware OS (All Platforms): 12.0 up to but not including 12.5.21
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://psirt.watchguard.com/CVE-2026-86101/ https://psirt.watchguard.com/CVE-2026-13046/ https://psirt.watchguard.com/CVE-2026-18145/ https://psirt.watchguard.com/CVE-2026-86104/ https://psirt.watchguard.com/CVE-2026-18105/ https://psirt.watchguard.com/CVE-2026-86128/ https://psirt.watchguard.com/CVE-2026-81433/ https://psirt.watchguard.com/CVE-2026-86136/ https://psirt.watchguard.com/CVE-2026-90441/ https://psirt.watchguard.com/CVE-2026-86105/ https://psirt.watchguard.com/CVE-2026-86132/ https://psirt.watchguard.com/CVE-2026-13224/ https://psirt.watchguard.com/CVE-2026-86133/

Vendor	HPE
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-76726, CVE-2026-76727, CVE-2026-76728, CVE-2026-76729, CVE-2026-76730, CVE-2026-76731, CVE-2026-76732, CVE-2026-76733, CVE-2026-76734, CVE-2026-76735, CVE-2026-76736, CVE-2026-76737, CVE-2026-76738)
Description	HPE 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. HPE advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Instant ON 3.4.1.0 and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw05150en_us&docLocale=en_US#vulnerability-summary-1

Vendor	Ubuntu
Severity	High, Medium, Low
Affected Vulnerability	Multiple Vulnerabilities
Description	Ubuntu 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. Ubuntu advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	Ubuntu 14.04, 16.04, 18.04, 20.04, 22.04, 24.04 and 26.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-8818-3 https://ubuntu.com/security/notices/USN-8819-3 https://ubuntu.com/security/notices/USN-8728-3 https://ubuntu.com/security/notices/USN-8816-2 https://ubuntu.com/security/notices/USN-8729-6

Vendor	OpenSSL
Severity	Low
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-84784, CVE-2026-84783, CVE-2026-84782, CVE-2026-77696, CVE-2026-75806, CVE-2026-75805, CVE-2026-75804, CVE-2026-72897, CVE-2026-54875, CVE-2026-54873, CVE-2026-54872, CVE-2026-42772, CVE-2026-35191, CVE-2026-35189)
Description	OpenSSL 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. OpenSSL advises to apply these security fixes at your earliest to protect your systems from potential threats.
Affected Products	OpenSSL versions: • from 4.0.0 before 4.0.3 • from 3.6.0 before 3.6.5 • from 3.5.0 before 3.5.9 • from 3.4.0 before 3.4.8 • from 3.0.0 before 3.0.23 • from 1.1.1 before 1.1.1zj • from 1.0.2 before 1.0.2zs
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://openssl-library.org/news/vulnerabilities/

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.

Financial Sector Computer Security Incident Response Team (FinCSIRT)

LankaPay Pvt Ltd, 'The Zenith', 161A, Dharmapala Mawatha, Colombo 07, Sri Lanka

Hotline: + 94 112039777