Advisory Alert

Alert Number: AAA20261023 **Date:** October 23, 2026

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Vendor	Severity	Vulnerability
Synology	**Critical**	Multiple Vulnerabilities
Dell	**Critical**	Multiple Vulnerabilities
Red Hat	**High**	Multiple Vulnerabilities
Check Point	**High**	Multiple Vulnerabilities
WatchGuard	**High**, **Medium**	Multiple Vulnerabilities

Description

Vendor	**Synology**
Severity	**Critical**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	Synology has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). Synology advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• PHP 8.4 - Versions prior to 8.4.27-0051 • PHP 8.3 - Versions prior to 8.3.36-0051 • PHP 8.2 - Versions prior to 8.2.35-0171 • PHP 8.1 - Versions prior to 8.1.34-0120 • PHP 8.0 - Versions prior to 8.0.30-0122 • PHP 7.4 - Versions prior to 7.4.33-0131 • PHP 7.3 - No fix will be provided as this version has reached end of life. • Mail Station - Versions prior to 30000002.3.19-20333 • Synology Calendar - Versions prior to 3.0.4-21435
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.synology.com/en-global/security/advisory/Synology_SA_26_14

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 Cyber Detect for PowerProtect - Versions prior to 8.13 • Dell VxRail Appliance - Versions prior to 9.1.100
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://www.dell.com/support/kbdoc/en-us/000524541/dsa-2026-475-security-update-for-dell-cyber-detect-for-powerprotect-for-php-vulnerabilities-cve-2026-109618-and-cve-2026-109619 • https://www.dell.com/support/kbdoc/en-us/000524406/dsa-2026-453-security-update-for-dell-vxrail-multiple-third-party-component-vulnerabilities

Vendor	**Red Hat**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38147, CVE-2026-64114, CVE-2026-64048, CVE-2026-64481, CVE-2026-64266, CVE-2026-64572, CVE-2026-68236, CVE-2026-68202, CVE-2026-68278, CVE-2026-68245, CVE-2026-68448, CVE-2026-80536, CVE-2026-80590, CVE-2026-80887, CVE-2026-89791, CVE-2026-89811, CVE-2026-93817, CVE-2026-97493, CVE-2026-68121, CVE-2026-74469, CVE-2026-80844, CVE-2026-81000, CVE-2026-11822, CVE-2026-11824, CVE-2026-54369, CVE-2026-5260, CVE-2026-58014, CVE-2026-58015, CVE-2026-99999)
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 Red Hat Enterprise Linux for x86_64 - Extended Update Support Red Hat Enterprise Linux for IBM z Systems Red Hat Enterprise Linux for IBM z Systems - Extended Update Support Red Hat Enterprise Linux for Power, little endian Red Hat Enterprise Linux for Power, little endian - Extended Update Support Red Hat Enterprise Linux for ARM 64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support Red Hat CodeReady Linux Builder for x86_64 Red Hat CodeReady Linux Builder for Power, little endian Red Hat CodeReady Linux Builder for ARM 64 Red Hat CodeReady Linux Builder for IBM z Systems Red Hat CodeReady Linux Builder for x86_64 - Extended Update Support Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support Red Hat Enterprise Linux Hidden Content for x86_64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates Red Hat Enterprise Linux for IBM z Systems - 4 years of updates Red Hat Enterprise Linux for Power, little endian - 4 years of support Red Hat Enterprise Linux for x86_64 - 4 years of updates Red Hat Enterprise Linux for x86_64 - Extended Life Cycle Red Hat Enterprise Linux for ARM 64 - Extended Life Cycle Red Hat Enterprise Linux for Power, little endian - Extended Life Cycle Red Hat Enterprise Linux for IBM z Systems - Extended Life Cycle Red Hat OpenShift Container Platform Red Hat OpenShift Container Platform for Power Red Hat OpenShift Container Platform for IBM Z and LinuxONE Red Hat OpenShift Container Platform for ARM 64 Red Hat Enterprise Linux Server - Extended Life Cycle Support Red Hat Enterprise Linux Server - Extended Life Cycle Support (for IBM z Systems) Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, big endian Red Hat Enterprise Linux Server - Extended Life Cycle Support for IBM Power, little endian
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2026:88477 • https://access.redhat.com/errata/RHSA-2026:82782 • https://access.redhat.com/errata/RHSA-2026:82811 • https://access.redhat.com/errata/RHSA-2026:88206

Vendor	**Check Point**
Severity	**High**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-109618, CVE-2026-109619)
Description	Check Point has released a security update addressing multiple vulnerabilities that exist in their products. **CVE-2026-109618:** PHP uses longjmp() for out-of-memory (OOM) errors to exit the current context and abort handling of the request. Some contexts may not properly account for this scenario and leave request memory in an uninitialized state before performing an allocation. The subsequent request cleanup procedure may read or branch on this memory. Multiple OOM strategies can consistently trigger this condition and lead to remote code execution (RCE). **CVE-2026-109619:** PHP has various global state that temporarily points into request memory. In some scenarios, global state may not be correctly reset, or may be repopulated after being reset. The global state may then refer to request memory even after it has been freed. Subsequent requests may read or branch on this stale state before it is fully initialized. Multiple strategies can trigger this condition and produce remote code execution (RCE). Check Point advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	• R81.20, R82, R82.10, R82.20 • R80, R80.10, R80.20, R80.30, R80.40, R81, R81.10 (all EoS) • Spark Firewalls R81.10.x, R82.00.x • Spark Firewalls R77.20.x, R80.20.x (all EoS)
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.checkpoint.com/results/sk/sk1000302

Vendor	**WatchGuard**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2026-96293, CVE-2026-115253)
Description	WatchGuard has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2026-96293:** A cleartext storage of sensitive information vulnerability in WatchGuard Endpoint Security's Full Disk Encryption feature for macOS allows a local, unprivileged user or process to obtain a managed computer's FileVault Personal Recovery Key by reading a persistently written diagnostic log file left readable by all local users. **CVE-2026-115253:** An incorrect permission assignment vulnerability in the WatchGuard Agent's log directory allows a local, authenticated non-administrative user to create, modify, append to, or delete the agent's log files and write other files into the directory. This allows an attacker to tamper with or destroy the agent's security logs and stage further local attacks by placing executable content in a directory owned by a privileged service. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	WatchGuard Agent: • MacOS - Versions prior to 1.17.24.0000 • Windows - Versions prior to 1.25.14.0000
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://psirt.watchguard.com/CVE-2026-96293/ • https://psirt.watchguard.com/CVE-2026-115253/

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.