Advisory Alert

Alert Number: AAA20250918 **Date:** September 18, 2025

Document Classification Level : Public Circulation Permitted | Public

Information Classification Level : TLP: WHITE

Overview

Product	Severity	Vulnerability
WatchGuard	**Critical**	Out of Bounds Write Vulnerability
Red Hat	**High**, **Medium**	Multiple Vulnerabilities
HPE	**High**, **Medium**	Multiple Vulnerabilities
Ubuntu	**High**, **Medium**	Multiple Linux kernel Vulnerabilities
cPanel	**Medium**	Multiple Vulnerabilities

Description

Affected Product	**WatchGuard**
Severity	**Critical**
Affected Vulnerability	Out of Bounds Write Vulnerability (CVE-2025-9242)
Description	WatchGuard has released security updates addressing an out of bounds write vulnerability that exists in their products. **CVE-2025-9242 -** An Out-of-bounds Write vulnerability in the WatchGuard Fireware OS iked process may allow a remote unauthenticated attacker to execute arbitrary code. This vulnerability affects both the mobile user VPN with IKEv2 and the branch office VPN using IKEv2 when configured with a dynamic gateway peer. If the Firebox was previously configured with the mobile user VPN with IKEv2 or a branch office VPN using IKEv2 to a dynamic gateway peer, and both of those configurations have since been deleted, that Firebox may still be vulnerable if a branch office VPN to a static gateway peer is still configured. WatchGuard advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Fireware OS 11.10.2 up to and including 11.12.4_Update1 Fireware OS 12.0 up to and including 12.11.3 and 2025.1
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://www.watchguard.com/wgrd-psirt/advisory/wgsa-2025-00015

Affected Product	**Red Hat**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-38052, CVE-2025-38352, CVE-2024-56721, CVE-2025-38079, CVE-2025-38084, CVE-2025-38085, CVE-2025-38137, CVE-2025-38159, CVE-2025-38292)
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 affected systems. Red Hat advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Red Hat Enterprise Linux for x86_64 10 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support 10.0 x86_64 Red Hat Enterprise Linux for IBM z Systems 10 s390x Red Hat Enterprise Linux for IBM z Systems - Extended Update Support 10.0 s390x Red Hat Enterprise Linux for Power, little endian 10 ppc64le Red Hat Enterprise Linux for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat Enterprise Linux for ARM 64 10 aarch64 Red Hat Enterprise Linux for ARM 64 - Extended Update Support 10.0 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 CodeReady Linux Builder for x86_64 - Extended Update Support 10.0 x86_64 Red Hat CodeReady Linux Builder for Power, little endian - Extended Update Support 10.0 ppc64le Red Hat CodeReady Linux Builder for IBM z Systems - Extended Update Support 10.0 s390x Red Hat CodeReady Linux Builder for ARM 64 - Extended Update Support 10.0 aarch64 Red Hat Enterprise Linux for ARM 64 - 4 years of updates 10.0 aarch64 Red Hat Enterprise Linux for IBM z Systems - 4 years of updates 10.0 s390x Red Hat Enterprise Linux for Power, little endian - 4 years of support 10.0 ppc64le Red Hat Enterprise Linux for x86_64 - 4 years of updates 10.0 x86_64 Red Hat Enterprise Linux for x86_64 - Extended Update Support Extension 8.6 x86_64 Red Hat Enterprise Linux Server for Power LE - Update Services for SAP Solutions 8.6 ppc64le Red Hat Enterprise Linux for x86_64 - Update Services for SAP Solutions 8.6 x86_64
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	• https://access.redhat.com/errata/RHSA-2025:16045 • https://access.redhat.com/errata/RHSA-2025:13598

Affected Product	**HPE**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-37122, CVE-2025-37123, CVE-2025-37124, CVE-2025-37125, CVE-2025-37126, CVE-2025-37127, CVE-2025-37128, CVE-2025-37129, CVE-2025-37130, CVE-2025-37131)
Description	HPE has released security updates addressing multiple vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to cause cross-site scripting, arbitrary command execution, authentication bypass, sensitive information disclosure. HPE advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	HPE Aruba Networking ClearPass Policy Manager • 6.12.x: ClearPass 6.12.5 and below • 6.11.x: ClearPass 6.11.12 and below HPE Aruba Networking EdgeConnect SD-WAN Gateways running (unless otherwise noted) • HPE Aruba Networking EdgeConnect SD-WAN Release Stream 9.5.x.x: 9.5.3.x and below • HPE Aruba Networking EdgeConnect SD-WAN Release Stream 9.4.x.x: 9.4.3.x and below
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04943en_us&docLocale=en_US https://support.hpe.com/hpesc/public/docDisplay?docId=hpesbnw04950en_us&docLocale=en_US

Affected Product	**Ubuntu**
Severity	**High**, **Medium**
Affected Vulnerability	Multiple Linux kernel vulnerabilities (CVE-2025-38350, CVE-2025-37752, CVE-2024-57996, CVE-2024-53131, CVE-2024-53130, CVE-2024-50202, CVE-2024-50051, CVE-2024-47685, CVE-2024-27074, CVE-2023-52477)
Description	Ubuntu has released security updates addressing multiple linux kernel vulnerabilities that exist in their products. These vulnerabilities could be exploited by malicious users to compromise affected systems. Ubuntu advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	Ubuntu 14.04 Ubuntu 16.04 Ubuntu 18.04
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://ubuntu.com/security/notices/USN-7755-1

Affected Product	**cPanel**
Severity	**Medium**
Affected Vulnerability	Multiple Vulnerabilities (CVE-2025-53859, CVE-2025-10148)
Description	cPanel has released security updates addressing multiple vulnerabilities that exist in their products. **CVE-2025-53859 -** NGINX Plus have a vulnerability in the ngx_mail_smtp_module that might allow an unauthenticated attacker to over-read NGINX SMTP authentication process memory; as a result, the server side may leak arbitrary bytes sent in a request to the authentication server. This issue happens during the NGINX SMTP authentication process and requires the attacker to make preparations against the target system to extract the leaked data. **CVE-2025-10148 -** curl's websocket code did not update the 32 bit mask pattern for each new outgoing frame as the specification says. Instead it used a fixed mask that persisted and was used throughout the entire connection. A predictable mask pattern allows for a malicious server to induce traffic between the two communicating parties that could be interpreted by an involved proxy (configured or transparent) as genuine, real, HTTP traffic with content and thereby poison its cache. That cached poisoned content could then be served to all users of that proxy. cPanel advises to apply security fixes at your earliest to protect systems from potential threats.
Affected Products	EasyApache 4 with all versions of ea-nginx through 1.26.3 and all versions of ea-libcurl through 8.15.0.
Officially Acknowledged by the Vendor	Yes
Patch/ Workaround Released	Yes
Reference	https://news.cpanel.com/easyapache4-v25-28-maintenance-and-security-release/

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.