VULNERABILITY BULLETINS

Critical Vulnerability in WatchGuard Firebox Firewalls (CVE-2025-9242)

TLP:WHITE

Sep 18, 2025

On September 17, 2025, WatchGuard released a security advisory regarding a critical vulnerability, tracked as CVE-2025-9242.

The security flaw affects an integral process of WatchGuard Fireware OS, which powers WatchGuard Firebox firewall appliances. Successful exploitation of the vulnerability allows remote unauthenticated attackers to execute arbitrary code on affected Firebox devices with specific configurations.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their level of risk to this vulnerability. WatchGuard has released patches to address this issue, and all affected organizations are strongly advised to apply the recommended updates immediately to prevent potential exploitation.

Analysis

The vulnerability, carrying a CVSS score of 9.3, stems from an out-of-bounds write flaw within the iked process of WatchGuard Fireware

OS, which underpins WatchGuard Firebox devices. WatchGuard Firebox appliances affected by CVE-2025-9242 include versions 11.x, 12.x, and 2025.1. The vulnerability primarily affects devices with a mobile user VPN or branch office VPN configured with a dynamic gateway peer using IKEv2. However, WatchGuard advises that a device may still be at risk if a branch office VPN to a static gateway peer is configured, even if the vulnerable configurations have been removed.

While there have been no public reports of active exploitation in the wild, the potential security implications are severe. An attacker who successfully exploits this flaw could gain a foothold on the network, bypass security controls, and move laterally to other systems. This could lead to a range of malicious activities, including data theft, a denial-of-service attack, or the deployment of ransomware.

Due to the nature of this vulnerability and the potential for critical security implications, it is imperative that organizations take immediate action. The flaw's ability to be exploited remotely without authentication makes it an attractive target for threat actors. Organizations can significantly reduce their attack surface and protect their network infrastructure from a potential compromise by applying the official patches or implementing the recommended mitigations.

Recommendations and Mitigations

Health-ISAC recommends organizations review and assess their level of risk to this vulnerability and implement the following:

- Upgrading affected WatchGuard Firebox appliances to a resolved version of the Fireware OS; these include:
    - 2025.1.1 for Fireware OS 2025.1
    - 12.11.4 for Fireware OS 12.x
    - 12.5.13 for Fireware OS 12.5.x (T15 & T35 models)

- 12.3.1_Update3 for the 12.3.1 FIPS-certified release

If immediate patching is not possible and the Firebox appliance is only configured with Branch Office VPN tunnels to static gateway peers, guidance for a temporary workaround is available here. Additional recommendations include reviewing the Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients Resources.

Reference(s)	bleepingcomputer, watchguard, watchguard 1, hhs

Alert ID 4ae4c000

View Alert

Share Feedback

was this helpful?  | 

Tags CVE-2025-9242, WatchGuard Firebox, WatchGuard Fireware OS

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**