Computer Emergency Response Team of Mauritius
Ministry of Information Technology, Communication and Innovation

CERT-MU Vulnerability Note

Critical Chrome Zero-Day and WatchGuard Firewall Vulnerability Demand Immediate Attention

Vulnerability Note: VN-2025-27

Date of Issue: 18 September 2025

Severity Rating: High

Systems Affected:

- Google Chrome browser (versions prior to 140.0.7339.185/.186)
- Chromium-based browsers (Microsoft Edge, Brave, Opera, Vivaldi)
- WatchGuard Firebox firewalls running Fireware OS 11.x, 12.x, and 2025.1

Description

Two critical security vulnerabilities have been disclosed that require immediate attention from organizations and users worldwide.

The first vulnerability (CVE-2025-10585) is a zero-day flaw in Google Chrome's V8 JavaScript and WebAssembly engine that has been actively exploited in the wild. Discovered by Google's Threat Analysis Group on September 16, 2025, this type confusion vulnerability can be weaponized by attackers to trigger unexpected software behavior, resulting in arbitrary code execution and program crashes. This marks the sixth Chrome zero-day vulnerability that has been actively exploited since the beginning of 2025.

The second critical vulnerability (CVE-2025-9242) affects WatchGuard Firebox firewalls and is caused by an out-of-bounds write weakness in the iked process. This vulnerability allows remote unauthenticated attackers to execute arbitrary code on vulnerable devices. The flaw specifically affects firewalls configured to use IKEv2 VPN, including both mobile user VPN and branch office VPN configurations. While not yet being exploited in the wild, the critical nature of this vulnerability makes it an attractive target for threat actors, especially given recent trends of firewall exploitation by ransomware gangs.

CVE Information

CVE-2025-10585
CVE-2025-9242

Mitigation

For Google Chrome Vulnerability (CVE-2025-10585):

1. Update Google Chrome immediately to version 140.0.7339.185/.186 for Windows and macOS, or 140.0.7339.185 for Linux

2. To verify updates: Navigate to More > Help > About Google Chrome and select Relaunch

3. Users of other Chromium-based browsers (Microsoft Edge, Brave, Opera, Vivaldi) should apply updates as soon as they become available

4. Consider implementing additional browser security controls and user awareness training

For WatchGuard Firebox Vulnerability (CVE-2025-9242):

1. Update affected Firebox devices to one of the following patched versions:

    - Fireware OS 12.3.1_Update3 (B722811)
    - Fireware OS 12.5.13
    - Fireware OS 12.11.4
    - Fireware OS 2025.1.1

2. For administrators who cannot immediately patch, implement the temporary workaround:

    - Disable dynamic peer BOVPNs
    - Add new firewall policies
    - Disable default system policies that handle VPN traffic

3. Review all VPN configurations, including those that may have been previously deleted

4. Monitor firewall logs for any signs of exploitation attempts

Postal address
Mauritian Computer Emergency Response Team (CERT-MU)
Ministry of Information Technology, Communication and Innovation
2nd Floor, Wing A,
Shri Atal Bihari Vajpayee Tower,
Cybercity Ebene