

Network Working Group
Internet-Draft
Intended status: Experimental
Expires: 9 May 2026

C. Ahrweiler
foxyfy.net
5 November 2025

Passive Hot Reload for Web Servers
draft-ahrweiler-hotreload-00

Abstract

This document defines a passive, file-based mechanism for automatic hot reloading of configuration files and TLS certificates in web servers. Unlike traditional web servers that require explicit reload commands, this design uses file modification time (mtime) to detect changes and reloads in memory automatically.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 9 May 2026.

Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

Table of Contents

1. Introduction	2
2. Mechanism	2
3. Security Considerations	2
4. Reference Implementation	2
5. Informative References	2
Author's Address	2

1. Introduction

Most web servers require manual intervention or explicit signals to reload configuration or TLS certificates. This document presents a passive strategy, based entirely on filesystem modification times, to perform reloads automatically and safely.

2. Mechanism

At startup, the server stores the current mtime of its configuration and TLS certificate files. A periodic timer (e.g. every 10 minutes) checks if those mtimes have changed. If so, the server reloads the updated configuration and certificates in memory without affecting active connections.

3. Security Considerations

Ensure proper file permissions to avoid unauthorized tampering. Always validate config and certificate contents before applying them. Avoid race conditions when reloading.

4. Reference Implementation

The FoxyFy web server implements this mechanism in Go. See [FOXYFY-SPEC] for full source and deployment notes.

5. Informative References

[FOXYFY-SPEC]
foxyfy.net, "FoxyFy Hot Reload (Full Specification)", URL
<https://foxyfy.net/spec/draft-foxyfy-hotreload-00.txt>, 5
November 2025.

Author's Address

Chris Ahrweiler
foxyfy.net
Email: info@foxyfy.net