

# Workspace overflow in HTTP/2 sessions *Security*

- [Overview](#)
- [Impact](#)
- [Status](#)
  - [Affected software versions](#)
  - [Resolved in](#)
- [Solution](#)
- [References](#)

Published April 9, 2026.

## Overview

The setup of an HTTP/2 session starts with a speculative HTTP/1 transport, and upon upgrading to h2 the HTTP/1 request is repurposed as stream zero. During the upgrade, a buffer allocation is made to reserve space to send frames to the client. This allocation would split the original workspace, and depending on the amount of prefetched data, the next fetch could perform a pipelining operation that would run out of workspace.

## Impact

In this scenario, a workspace overflow would result in a panic, and could be used as a Denial of Service attack vector by malicious clients.

## Status

### Affected software versions

- Varnish Enterprise 6.0 series from version 6.0.14r1 up to and including 6.0.16r10.

- Varnish Cache 9.0.0

## Resolved in

- Varnish Enterprise 6.0.16r11
- Varnish Cache 9.0.1

## Solution

The recommended solution is to upgrade Varnish to one of the versions where this issue has been resolved, and then ensure that Varnish is restarted.

To avoid fragmenting the h2 session receive buffer, the send buffer is now allocated from `workspace_thread` (similarly to HTTP/1 delivery). This ensures that any amount of data received in `workspace_client` before the upgrade from HTTP/1 to h2 will still fit inside the workspace after the upgrade. This is guaranteed because the only remaining purpose of `workspace_client` in the h2 session thread is to serve as a receive buffer.

## References

- CVE: pending

---

### Manuals

[Varnish Enterprise](#)

[Varnish Cloud](#)

[Varnish Controller](#)

[Varnish High Availability](#)

[Varnish Custom Statistics](#)

[Varnish WAF](#)

[Varnish Broadcaster](#)

[Varnish Helm Chart](#)

[Packages](#)

[Docker](#)

[Varnish Otel](#)

## News

[Denial Of Service in shared VCL deployments](#)

[Workspace overflow in HTTP/2 sessions](#)

[HTTP/1 absolute URL parsing deficiency](#)

[Varnish Controller Helm Charts 1.7.7](#)

[Varnish Broadcaster 1.6.3](#)

[News archive](#)

[Cookie Settings](#)

[Privacy Policy](#)

[Contact Us](#)

[Press](#)

[Branding](#)

©Varnish Software, Wallingatan 12, 111 60 Stockholm, Organization nr. 556805-6203