VARNISH SOFTWARE

Search

Denial Of Service in shared VCL deployments *Security*

Published April 9, 2026.

Overview

The `headerplus.write_req0()` function from `vmod_headerplus` updates the underlying `req0`, which is normally the original read-only request from which `req` is derived (readable and writable from VCL).

This is useful in the active VCL, after amending `req`, to prepare a refined `req0` before switching to a different VCL with the `return (vcl(<label>))` action. This is for example how the Varnish Controller operates shared VCL deployments.

If the amended `req` contained too many header fields for `req0`, this would have resulted in a workspace overflow that would in turn trigger a panic and crash the Varnish Enterprise server.

Impact

This could be used as a Denial of Service attack vector by malicious clients.

Status

Affected software versions

- Varnish Enterprise 6.0 series from version 6.0.9r5 up to and including 6.0.16r11.

Resolved in

- Varnish Enterprise 6.0.16r12

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.

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