Apache HTTP Server fixes critical HTTP/2 remote code execution flaw (CVE-2026-119618)



Apache has patched CVE-2026-119618, a race condition in mod_http2 that lets an unauthenticated attacker run code remotely. Affected servers should be updated, or HTTP/2 disabled until patching is possible.

- CVE-2026-119618 is a race condition in mod_http2 that corrupts heap memory and can lead to remote code execution without authentication.
- Affected: Apache HTTP Server 2.4.55 through 2.4.70, and standalone mod_h2 2.0.8 through 2.0.42.
- Exploitation requires HTTP/2 to be enabled, which is off by default.
- Wiz telemetry shows 64% of cloud environments hold vulnerable resources, about half of them publicly exposed; Wiz knows of no public exploits or attacks yet.
- The latest release also fixes CVE-2026-106023 in mod_md and a low-severity flaw,

> CVE-2026-109163, in mod_vhost_alias.

The Apache Software Foundation has released a fix for a critical vulnerability in the HTTP/2 module of Apache HTTP Server, tracked as CVE-2026-119618. An unauthenticated attacker could exploit it to achieve remote code execution.

What the flaw is

The issue is a race condition in the mod_http2 module, caused by improper synchronization of concurrent threads sharing resources. It can corrupt heap memory and, according to Wiz researchers, be leveraged to run arbitrary commands with the privileges of the web server process. It affects Apache HTTP Server 2.4.55 through 2.4.70 and standalone mod_h2 2.0.8 through 2.0.42. The flaw was found by Anthropic's OSS Scanner and Google Cloud's Vulnerability Research teams.

Exposure and current status

Wiz telemetry indicates that 64% of cloud environments contain vulnerable resources, and roughly half of those have publicly exposed instances. These figures do not consider configuration: exploitation requires HTTP/2 to be enabled, and it is off by default. watchTowr confirmed this condition and advises patching immediately or disabling h2 until patching is done.

Wiz rates the severity as critical, though no official score exists. It is not aware of public exploits or attacks, but warns this could change soon. The same release also fixes CVE-2026-106023, a null pointer dereference in mod_md, and CVE-2026-109163, a low-severity data overwrite flaw in mod_vhost_alias.

Institutions running Apache on internet-facing systems should confirm versions and HTTP/2 settings promptly.

What to do now

1. Inventory all Apache HTTP Server instances and standalone mod_h2 deployments, including cloud and third-party hosted ones, and record versions.
2. Update affected servers to the latest Apache HTTP Server release, prioritizing internet-facing systems.
3. Where patching cannot happen immediately, disable HTTP/2 until the update is applied.
4. Check configurations to determine whether HTTP/2 is enabled on each server.
5. Monitor web servers for unusual process activity and unexpected commands, and review logs for signs of compromise.
6. Record the exposure and remediation in your vulnerability management process for ECC and SAMA CSF evidence.