Critical Apache HTTP/2 flaw (CVE-2026-119618) allows remote code execution; update to 2.4.71



A critical flaw in Apache HTTP Server's mod_http2 module, CVE-2026-119618, can let a remote attacker run code on the server. Versions 2.4.55 through 2.4.70 are affected; 2.4.71 contains the fix.

- CVE-2026-119618 is a critical flaw in the mod_http2 module of Apache HTTP Server.
- A remote attacker can run code on the server.
- Affected versions are 2.4.55 through 2.4.70; version 2.4.71 fixes the issue.
- Only servers with HTTP/2 enabled are affected, according to Red Hat.
- Red Hat ships Apache HTTP Server as part of Red Hat Enterprise Linux.

What was reported

A critical vulnerability has been disclosed in mod_http2, the HTTP/2 module of Apache HTTP Server. Tracked as **CVE-2026-119618**, it can allow a remote attacker to run code on an affected server.

The flaw affects versions 2.4.55 through 2.4.70. The Apache project has released version 2.4.71, which fixes it. According to Red Hat, which distributes the server as part of Red Hat Enterprise Linux, only servers with HTTP/2 enabled are affected.

Who should pay attention

Any institution running Apache HTTP Server in the affected version range should check whether HTTP/2 is enabled. This includes internet-facing web servers and any internal systems that rely on Apache, including those delivered through Red Hat Enterprise Linux packages.

The source text available to us does not detail the exact exploitation conditions or confirm active exploitation, so teams should rely on the vendor advisories for those specifics.

Recommended approach

The priority is to establish exposure quickly: find the Apache instances, confirm their versions, and check whether HTTP/2 is turned on. Then move to the fixed release, or to the corresponding package update from your Linux vendor, through your normal emergency change process.

What to do now

1. Inventory all Apache HTTP Server instances and record their versions, including those installed via Red Hat Enterprise Linux.
2. Check whether HTTP/2 (mod_http2) is enabled on each instance in the 2.4.55–2.4.70 range.
3. Upgrade to Apache HTTP Server 2.4.71 or apply the equivalent vendor package update through emergency change management.
4. Prioritise internet-facing servers first, then internal ones.
5. Review the vendor advisories from Apache and Red Hat for mitigation details and record the remediation for compliance evidence.