Critical Heap Corruption and Remote Code Execution Vulnerability in Apache HTTP/2 (CVE-2026-119618)

Nov 13, 2026

WHITE

View Alert

The Apache Software Foundation has fixed a critical vulnerability, tracked as **CVE-2026-119618**, in the *mod_http2* module of the **Apache HTTP Server**.

Health-ISAC provides this information to increase situational awareness and encourage organizations to assess their risk exposure to the vulnerability.

Additional Info

Analysis:

The Apache Software Foundation recently released updates to address a critical vulnerability, tracked as **CVE-2026-119618** (CVSS score of **9.8**), within the *mod_http2* module of the widely deployed **Apache HTTP Server**.

Identified by Anthropic's OSS Scanner and Google Cloud's Vulnerability Research teams, the issue involves improper synchronization during concurrent thread execution, which causes a race condition and heap memory corruption. This flaw affects server versions **2.4.55 through 2.4.70** and standalone *mod_h2* versions **2.0.8 through 2.0.42** where HTTP/2 functionality is actively enabled, alongside two secondary flaws in *mod_md* and *mod_vhost_alias*.

From a health sector security perspective, this vulnerability warrants close attention because open-source web servers commonly host patient portals, telehealth interfaces, and clinical administrative tools. Although HTTP/2 is disabled by default, organizations that enable it to optimize web performance for external-facing applications face potential exposure. An unauthenticated actor exploiting this race condition could execute arbitrary code with web server privileges, potentially compromising the confidentiality of electronic health records or disrupting the availability of essential digital patient services.

While cloud telemetry from Wiz indicates that many environments contain affected server versions, actual risk depends heavily on specific server configurations and public internet exposure. Health sector IT teams should evaluate their web infrastructure footprints promptly to mitigate potential operational disruptions before exploitation attempts materialize.

Recommendations:

Health-ISAC recommends organizations review and assess their risk exposure to these vulnerabilities and implement the following:

- Apply the latest Apache HTTP Server patches immediately to update affected instances beyond version 2.4.70 and standalone *mod_h2* beyond version 2.0.42.
- Audit public-facing healthcare web servers, patient portals, and cloud environments to identify where HTTP/2 is actively enabled.
- Temporarily disable the *mod_http2* module as a workaround if immediate patching conflicts with clinical operational schedules or maintenance windows.
- Monitor web server logs and network traffic for unusual behavior, unexpected process crashes, or signs of unauthorized command execution.
- **Review the Health Industry Cybersecurity Practices (HICP):** Managing Threats and Protecting Patients Resources.

<hr size=1 width="100%" align=center>

Alert Id	baaa76a1
Category	Vulnerability Bulletins
References	apache hhs bleepingcomputer wiz

Tags	CVE-2026-119618, Apache HTTP, heap corruption, HTTP/2, Remote Code Execution

---

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Access the Health-ISAC Threat Intelligence Portal
Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments
Please email us at toc@h-isac.org

Please provide your feedback

Like | Dislike

Download the App
Available on iOS, Android and Web

Download on the App Store | Get it on Google Play

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**
Health-ISAC is an invite only platform. Please DO NOT forward this email to anyone. If you are not supposed to receive this email, please report to **toc@h-isac.org**

--
You received this message because you are subscribed to the Google Groups "TLP Green - Health-ISAC Partners" group.
To unsubscribe from this group and stop receiving emails from it, send an email to health-isac-partners+unsubscribe@h-isac.org.
To view this discussion visit https://groups.google.com/a/h-isac.org/d/msgid/health-isac-partners/010001a1d32fd2d1-d803470a-e05a-43f5-9e03-79669b634ada-000000%40email.amazonses.com.