An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611120264

NCSC Advisory

Critical RCE Vulnerability in Apache HTTP Server

CVE-2026-119618

12th, November 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-119618

Published: 2026-11-11

Vendor: Apache Software Foundation

Product: Apache HTTP Server

CVSS Score[1]: 9.8

Products Affected

Product	Version
Apache HTTP Server	2.4.55 <= 2.4.70
mod_h2	2.0.8 <= 2.0.42

Impact

Concurrent Execution using Shared Resource with Improper Synchronization vulnerability in Apache HTTP Server's mod_http2 in assign_headers() can lead to RCE.

A remote attacker who can reach the web server could exploit this flaw to execute arbitrary commands on the server without any authentication, potentially leading to a complete takeover of the affected system, unauthorised access to sensitive data, and service disruption.

Only servers that have HTTP/2 enabled are affected; servers configured to serve only HTTP/1.1 are not vulnerable.

Common Weakness Enumeration (CWE)[2]: CWE-362: Concurrent Execution using Shared Resource with Improper Synchronization

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from Apache Software Foundation.

- https://nvd.nist.gov/vuln/detail/CVE-2026-119618
- https://www.cve.org/CVERecord?id=CVE-2026-119618
- https://httpd.apache.org/security/vulnerabilities_24.html
- http://www.openwall.com/lists/oss-security/2026/11/11/13
- https://access.redhat.com/security/cve/cve-2026-119618
- https://www.wiz.io/blog/cve-2026-119618-rce-apache-http-server-vulnerability
- https://github.com/microsoft/azurelinux/pull/20165
- https://bugs.gentoo.org/986161
- https://github.com/AlmaLinux/updates/issues/4252