Apache 2.4 security advisory

Article Number: 2042 | Rating: Unrated | Last Updated: Tue, May 5, 2026 at 3:10 PM

On 4 May 2026, the Apache Software Foundation released version 2.4.67 of Apache HTTP Server, which addresses eleven CVEs. . **What's been disclosed** **CVE-2026-23918 (CVSS 8.8, High)** - A double free in Apache's HTTP/2 implementation that may allow remote code execution via a crafted "early reset" frame. This affects only Apache HTTP Server 2.4.66 — earlier versions are not affected by this specific bug. **CVE-2026-24072 (Moderate)** - A privilege escalation issue in mod_rewrite expression evaluation. A user able to write .htaccess files can read files with the privileges of the Apache process. This is most relevant if you run shared hosting, reseller setups, or any environment where multiple users have write access to web directories. This affects Apache 2.4.66 and earlier. The remaining nine are lower-severity issues in mod_proxy_ajp, mod_md, mod_dav_lock, mod_authn_socache, and mod_auth_digest. All eleven are addressed by the same upgrade — see the Apache advisory linked below for the full list. **Am I affected? Both vulnerabilities affect VPS and dedicated servers running Apache 2.4.66 or earlier. If you are already on Apache 2.4.67 or later, you are not affected. What you need to do**: For cPanel users Update EasyApache 4 via SSH using the appropriate command for your OS. On AlmaLinux: dnf clean all dnf makecache dnf -y update ea-apache* On Ubuntu: apt update apt install --only-upgrade "ea-apache24*" This upgrades Apache to version 2.4.67. Full cPanel advisory and patch notes: https://support.cpanel.net/hc/en-us/articles/40229402602519-Security-CVE-2026-23918 For Plesk users 1. Check your Apache version via SSH: httpd -v or apache2 -v 2. Apply system updates via your OS package manager: dnf update or apt upgrade 3. Monitor the Plesk Change Log at https://docs.plesk.com for a dedicated advisory as updates become available Machines without control panel If you are using a machine without a control panel or an alternative 3rd party control panel, please consult your OS or control panel documentation on the best way to upgrade Apache. **Further reading** Apache security advisories: https://httpd.apache.org/security/vulnerabilities_24.html CVE-2026-23918: https://www.cve.org/CVERecord?id=CVE-2026-23918 CVE-2026-24072: https://www.cve.org/CVERecord?id=CVE-2026-24072 cPanel advisory: https://support.cpanel.net/hc/en-us/articles/40229402602519

Posted - Tue, May 5, 2026 at 3:01 PM.

Online URL: https://www.heartinternet.uk/support/article/apache-2-4-security-advisory.html