



CVE-2023-45802

[MITRE](#)[NVD](#)[CVE.ORG](#)[Print: PDF !\[\]\(e3f8612927870f2e0f9f5989e6dd3064_img.jpg\)](#)

Summary

CVE	CVE-2023-45802
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-23 07:15:00 UTC
Updated	2023-11-07 05:15:00 UTC
Description	When a HTTP/2 stream was reset (RST frame) by a client, there was a time window were the request's memory resources

Risk And Classification

Problem Types: CWE-400

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Operating System	Fedoraproject	Fedora	38	All	All	All

References

Reference	Source	Link
[SECURITY] Fedora 39 Update: mod_http2-2.0.25-1.fc39 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
[SECURITY] Fedora 38 Update: mod_http2-2.0.25-1.fc38 - package-announce - Fedora Mailing-Lists	MISC	lists.fedoraproject.org
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	MISC	httpd.apache.org
[SECURITY] Fedora 37 Update: mod_http2-2.0.25-1.fc37 - package-announce - Fedora Mailing-Lists		lists.fedoraproject.org
October 2023 Apache HTTP Server Vulnerabilities in NetApp Products NetApp Product Security	MISC	security.netapp.com
CVE Program record	CVE.ORG	www.cve.org
NVD vulnerability detail	NVD	nvd.nist.gov

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150737](#) Apache HTTP Server Prior to 2.4.58 Multiple Security Vulnerabilities

199940 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-6506-1)
242553 Red Hat Update for JBoss Core Services (RHSA-2023:7625)
284656 Fedora Security Update for mod_http2 (FEDORA-2023-0259c3f26f)
284710 Fedora Security Update for mod_http2 (FEDORA-2023-c0c6a91330)
285180 Fedora Security Update for mod_http2 (FEDORA-2023-492b7be466)
296106 Oracle Solaris 11.4 Support Repository Update (SRU) 64.157.2 Missing (CPUOCT2023)
356549 Amazon Linux Security Advisory for httpd24 : ALAS-2023-1877
356605 Amazon Linux Security Advisory for httpd : ALAS2-2023-2322
356896 Amazon Linux Security Advisory for httpd : ALAS2023-2023-433
503432 Alpine Linux Security Update for apache2
505847 Alpine Linux Security Update for apache2
673364 EulerOS Security Update for httpd (EulerOS-SA-2023-3273)
673411 EulerOS Security Update for httpd (EulerOS-SA-2023-3334)
673591 EulerOS Security Update for httpd (EulerOS-SA-2024-1085)
673592 EulerOS Security Update for httpd (EulerOS-SA-2023-3302)
673720 EulerOS Security Update for httpd (EulerOS-SA-2024-1273)
673736 EulerOS Security Update for httpd (EulerOS-SA-2024-1061)
674081 EulerOS Security Update for httpd (EulerOS-SA-2023-3245)
691333 Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (f923205f-6e66-11ee-85eb-84a93843eb75)
907568 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (31611-1)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)