



CVE-2023-25690

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

Summary

CVE	CVE-2023-25690
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-03-07 16:15:00 UTC
Updated	2024-01-02 16:15:00 UTC
Description	Some mod_proxy configurations on Apache HTTP Server versions 2.4.0 through 2.4.55 allow a HTTP Request Smuggling

Risk And Classification

Problem Types: CWE-444

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All

References

Reference	Source	Link	T
packetstormsecurity.com/files/176334/Apache-2.4.55-mod_proxy-HTTP-Request-Smuggling.html		packetstormsecurity.com	
[SECURITY] [DLA 3401-1] apache2 security update	MISC	lists.debian.org	
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	MISC	httpd.apache.org	
Apache HTTPD: Multiple Vulnerabilities (GLSA 202309-01) — Gentoo security	MISC	security.gentoo.org	
CVE Program record	CVE.ORG	www.cve.org	c
NVD vulnerability detail	NVD	nvd.nist.gov	c

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[150660](#) Apache HTTP Server Prior to 2.4.56 Multiple Security Vulnerabilities

[160534](#) Oracle Enterprise Linux Security Update for httpd (ELSA-2023-1593)

[160533](#) Oracle Enterprise Linux Security Update for httpd (ELSA-2023-1593)

160539 Oracle Enterprise Linux Security Update for httpd and mod_http2 (ELSA-2023-1670)
160540 Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2023-1673)
181660 Debian Security Update for apache2 (DSA 5376-1)
181753 Debian Security Update for apache2 (DLA 3401-1)
184656 Debian Security Update for apache2 (CVE-2023-25690)
199231 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5942-1)
199481 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerability (USN-5942-2)
241313 Red Hat Update for httpd (RHSA-2023:1593)
241314 Red Hat Update for httpd:2.4 (RHSA-2023:1596)
241323 Red Hat Update for httpd:2.4 (RHSA-2023:1597)
241330 Red Hat Update for httpd and mod_http2 (RHSA-2023:1670)
241331 Red Hat Update for httpd:2.4 (RHSA-2023:1673)
241372 Red Hat Update for httpd and mod_http2 (RHSA-2023:1916)
241556 Red Hat Update for httpd24-httpd (RHSA-2023:3292)
241574 Red Hat Update for JBoss Core Services (RHSA-2023:3354)
241595 Red Hat Update for httpd:2.4 (RHSA-2023:1672)
241656 Red Hat Update for httpd:2.4 (RHSA-2023:1547)
283776 Fedora Security Update for httpd (FEDORA-2023-54dae7b78a)
283818 Fedora Security Update for httpd (FEDORA-2023-7df48f618b)
284249 Fedora Security Update for httpd (FEDORA-2023-7d14cdec4a)
354828 Amazon Linux Security Advisory for httpd : ALAS2-2023-1989
354845 Amazon Linux Security Advisory for httpd24 : ALAS-2023-1711
355276 Amazon Linux Security Advisory for httpd : ALAS2023-2023-136
378328 IBM Hypertext Transfer Protocol (HTTP) Server Bypass Access Control Vulnerability (6963650)
378424 Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2023:0018)
378450 F5 BIG-IP Apache Vulnerability (K000133098)
378489 NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Denial of Service (DoS) Vulnerability (NTAP-20230316-0007)
378677 Oracle Hypertext Transfer Protocol Server (HTTP Server) Server Multiple Vulnerabilities (CPUJUL2023)
500070 Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2023:0018)

502676 Alpine Linux Security Update for apache2
503859 Alpine Linux Security Update for apache2
672896 EulerOS Security Update for httpd (EulerOS-SA-2023-1805)
672908 EulerOS Security Update for httpd (EulerOS-SA-2023-1823)
672999 EulerOS Security Update for httpd (EulerOS-SA-2023-1847)
673013 EulerOS Security Update for httpd (EulerOS-SA-2023-1872)
673063 EulerOS Security Update for httpd (EulerOS-SA-2023-2191)
673065 EulerOS Security Update for httpd (EulerOS-SA-2023-2148)
673142 EulerOS Security Update for httpd (EulerOS-SA-2023-2271)
673150 EulerOS Security Update for httpd (EulerOS-SA-2023-2295)
691094 Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (8edeb3c1-bfe7-11ed-96f5-3497f65b111b)
730758 Apache Hypertext Transfer Protocol (HTTP) Server Request Smuggling Vulnerability
753799 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2023:0764-1)
753813 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2023:0799-1)
753814 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2023:0803-1)
753845 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2023:1573-1)
906680 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (25605-3)
906720 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (25614-1)
940978 AlmaLinux Security Update for httpd:2.4 (ALSA-2023:1673)
940983 AlmaLinux Security Update for httpd and mod_http2 (ALSA-2023:1670)
960909 Rocky Linux Security Update for httpd:2.4 (RLSA-2023:1673)
960910 Rocky Linux Security Update for httpd and mod_http2 (RLSA-2023:1670)

© [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](#)