CVE-2021-34798

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-34798
State	PUBLIC
Assigner	security@apache.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-09-16 15:15:00 UTC
Updated	2023-11-07 03:36:00 UTC
Description	Malformed requests may cause the server to dereference a NULL pointer. This issue affects Apache HTTP Server 2.4.48 a

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update
Application	Apache	Http Server	All	All
Operating System	Broadcom	Brocade Fabric Operating System Firmware	-	All
Operating System	Debian	Debian Linux	10.0	All
Operating System	Debian	Debian Linux	11.0	All
Operating System	Debian	Debian Linux	9.0	All
Operating System	Fedoraproject	Fedora	34	All
Operating System	Fedoraproject	Fedora	35	All
Application	Netapp	Cloud Backup	-	All
Application	Netapp	Clustered Data Ontap	-	All
Application	Netapp	Storagegrid	-	All
Application	Oracle	Communications Cloud Native Core Network Function Cloud Native Environment	1.10.0	All
Application	Oracle	Enterprise Manager Base Platform	13.4.0.0	All
Application	Oracle	Enterprise Manager Base Platform	13.5.0.0	All
Application	Oracle	Http Server	12.2.1.3.0	All
Application	Oracle	Http Server	12.2.1.4.0	All
Application	Oracle	Instantis Enterprisetrack	17.1	All
Application	Oracle	Instantis Enterprisetrack	17.2	All

Application	Oracle	Instantis Enterprisetrack	17.3	All
Application	Oracle	Peoplesoft Enterprise Peopletools	8.58	All
Application	Oracle	Zfs Storage Appliance Kit	8.8	All
Application	Siemens	Ruggedcom Nms	All	All
Application	Siemens	Sinec Nms	All	All
Application	Siemens	Sinema Remote Connect Server	All	All
Application	Siemens	Sinema Server	14.0	-
Application	Tenable	Tenable.sc	All	All

References

Reference
September 2021 Apache HTTP Server Vulnerabilities in NetApp Products | NetApp Product Security
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project
Apache HTTPD: Multiple Vulnerabilities (GLSA 202208-20) — Gentoo security
[R1] Stand-alone Security Patch Available for Tenable.sc versions 5.16.0 to 5.19.1: Patch 202110.1 - Security Advisory | Tenable®
[SECURITY] Fedora 35 Update: httpd-2.4.49-1.fc35 - package-announce - Fedora Mailing-Lists
[httpd-users] 20210923 Re: [users@httpd] Re: [External] : [users@httpd] 2.4.49 security fixes: more info
[httpd-users] 20210923 [users@httpd] 2.4.49 security fixes: more info
[SECURITY] Fedora 34 Update: httpd-2.4.49-1.fc34 - package-announce - Fedora Mailing-Lists
Pony Mail!
Oracle Critical Patch Update Advisory - April 2022
Debian -- Security Information -- DSA-4982-1 apache2
Pony Mail!
Oracle Critical Patch Update Advisory - January 2022
Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products: November 2021
Pony Mail!
Pony Mail!
Security Bulletin - ePolicy Orchestrator update addresses multiple product vulnerabilities (CVE-2022-0842, CVE-2022-0857, CVE-2022-0858,
[httpd-users] 20210923 Re: [users@httpd] 2.4.49 security fixes: more info
[SECURITY] Fedora 35 Update: httpd-2.4.49-1.fc35 - package-announce - Fedora Mailing-Lists
[SECURITY] [DLA 2776-1] apache2 security update
cert-portal.siemens.com/productcert/pdf/ssa-685781.pdf
[httpd-users] 20210923 [users@httpd] Re: [External] : [users@httpd] 2.4.49 security fixes: more info
[SECURITY] Fedora 34 Update: httpd-2.4.49-1.fc34 - package-announce - Fedora Mailing-Lists
CVE Program record

NVD vulnerability detail

Vendor Comments And Credit

Discovery Credit

LEGACY: The issue was discovered by the Apache HTTP security team

Legacy QID Mappings

150399 Apache HTTP Server Multiple Vulnerabilities (CVE-2021-34798,CVE-2021-39275)

159570 Oracle Enterprise Linux Security Update for httpd (ELSA-2021-9619)

159594 Oracle Enterprise Linux Security Update for httpd (ELSA-2022-0143)

159609 Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-9005)

159711 Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-0891)

178815 Debian Security Update for apache2 (DLA 2776-1)

178819 Debian Security Update for apache2 (DSA 4982-1)

182064 Debian Security Update for apache2 (CVE-2021-34798)

198516 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5090-1)

240007 Red Hat Update for httpd (RHSA-2022:0143)

240149 Red Hat Update for httpd:2.4 (RHSA-2022:0891)

240698 Red Hat Update for httpd24-httpd (RHSA-2022:6753)

257148 CentOS Security Update for httpd (CESA-2022:0143)

281910 Fedora Security Update for Hypertext Transfer Protocol Daemon (HTTPd) (FEDORA-2021-dce7e7738e)

352857 Amazon Linux Security Advisory for httpd24: ALAS-2021-1543

352858 Amazon Linux Security Advisory for httpd: ALAS2-2021-1716

375963 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Apache HTTPD Vulnerability (K72382141)

375988 Apache Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities

376041 IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6493841)

376381 IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6493845,6493841)

376961 NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Disclosure of Sensitive Information Vulnerability (NTAP-20211008-0004)

377218 Alibaba Cloud Linux Security Update for httpd (ALINUX2-SA-2022:0004)

377378 Alibaba Cloud Linux Security Update for httpd:2.4 (ALINUX3-SA-2022:0017)

378433 Oracle Hypertext Transfer Protocol Server (HTTP Server) Server Multiple Vulnerabilities (CPUAPR2023)

38856 Cisco TelePresence Video Communication Server (VCS) Apache HTTP Server Vulnerability (cisco-sa-apache-httpd-2.4.49-VWL69sWQ)

500022 Alpine Linux Security Update for apache2

503713 Alpine Linux Security Update for apache2

590870 Mitsubishi Electric MELSOFT iQ AppPortal Multiple Vulnerabilities (ICSA-22-132-02)

591221 Siemens SINEC NMS and SINEMA Server Multiple Vulnerabilities (SSA-685781 V1.1)

671157 EulerOS Security Update for httpd (EulerOS-SA-2021-2803)

671166 EulerOS Security Update for httpd (EulerOS-SA-2021-2915)

671168 EulerOS Security Update for httpd (EulerOS-SA-2021-2923)

671190 EulerOS Security Update for httpd (EulerOS-SA-2021-2931)

671266 EulerOS Security Update for httpd (EulerOS-SA-2022-1167)

671293 EulerOS Security Update for httpd (EulerOS-SA-2022-1206)

671333 EulerOS Security Update for httpd (EulerOS-SA-2022-1225)

690025 Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (882a38f9-17dd-11ec-b335-d4c9ef517024)

710595 Gentoo Linux Apache HTTPD Multiple Vulnerabilities (GLSA 202208-20)

730209 Apache Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities

751198 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2021:3299-1)

751216 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2021:3335-1)

751279 OpenSUSE Security Update for apache2 (openSUSE-SU-2021:3522-1)

751314 OpenSUSE Security Update for apache2 (openSUSE-SU-2021:1438-1)

87470 IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6493841)

900386 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (5487)

901054 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (6484-1)

940471 AlmaLinux Security Update for httpd:2.4 (ALSA-2022:0891)

960723 Rocky Linux Security Update for httpd:2.4 (RLSA-2022:0891)

CVE.report and Source URL Uptime Status status.cve.report