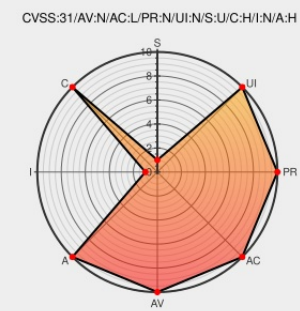
CVE-2022-28615

Published on: Not Yet Published

Last Modified on: 08/24/2022 06:17:00 PM UTC

CVE-2022-28615

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Http Server from Apache contain the following vulnerability:

Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond bounds in ap_strcmp_match() when provided with an extremely large input buffer. While no code distributed with the server can be coerced into such a call, third-party modules or lua scripts that use ap_strcmp_match() may hypothetically be affected.

CVE-2022-28615 has been assigned by security@apache.org to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **Apache Software Foundation** - **Apache HTTP Server** version **<= 2.4.53**

CVSS3 Score: 9.1 - CRITICAL

Attack Vector	Attack Complexity	Privileges Required	User Interaction
NETWORK	LOW	NONE	NONE
Scope	**Confidentiality Impact**	**Integrity Impact**	**Availability Impact**
UNCHANGED	HIGH	NONE	HIGH

CVSS2 Score: 6.4 - MEDIUM

Access Vector	Access Complexity	Authentication
NETWORK	LOW	NONE
Confidentiality Impact	**Integrity Impact**	**Availability Impact**
PARTIAL	NONE	PARTIAL

CVE References

Description	Tags	Link
Apache HTTPD: Multiple Vulnerabilities (GLSA 202208-	security.gentoo.org	GENTOO GLSA-202208-20

20) — Gentoo security	text/html	
[SECURITY] Fedora 36 Update: httpd-2.4.54-3.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-e620fb15d5
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	httpd.apache.org text/html	MISC httpd.apache.org/security/vulnerabilities_24.html
[SECURITY] Fedora 35 Update: httpd-2.4.54-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-b54a8dee29
June 2022 Apache HTTP Server Vulnerabilities in NetApp Products | NetApp Product Security	security.netapp.com text/html	CONFIRM security.netapp.com/advisory/ntap-20220624-0005/
oss-security - CVE-2022-28615: Apache HTTP Server: Read beyond bounds in ap_strcmp_match()	www.openwall.com text/html	MLIST [oss-security] 20220608 CVE-2022-28615: Apache HTTP Server: Read beyond bounds in ap_strcmp_match()

Related QID Numbers

150539 Apache HTTP Server 2.4.53 Multiple Vulnerabilities

160250 Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-7647)

160309 Oracle Enterprise Linux Security Update for httpd (ELSA-2022-8067)

180837 Debian Security Update for apache2 (CVE-2022-28615)

198838 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5487-1)

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

240854 Red Hat Update for httpd:2.4 (RHSA-2022:7647)

240885 Red Hat Update for httpd security (RHSA-2022:8067)

240996 Red Hat Update for JBoss Core Services (RHSA-2022:8840)

282882 Fedora Security Update for httpd (FEDORA-2022-e620fb15d5)

282903 Fedora Security Update for httpd (FEDORA-2022-b54a8dee29)

296082 Oracle Solaris 11.4 Support Repository Update (SRU) 48.126.1 Missing (CPUJUL2022)

353971 Amazon Linux Security Advisory for httpd24 : ALAS-2022-1607

353988 Amazon Linux Security Advisory for httpd : ALAS2-2022-1812

354482 Amazon Linux Security Advisory for httpd : ALAS2022-2022-202

354513 Amazon Linux Security Advisory for httpd : ALAS2022-2022-110

354577 Amazon Linux Security Advisory for httpd : ALAS2022-2022-202

355264 Amazon Linux Security Advisory for httpd : ALAS2023-2023-072

376754 F5 BIG-IP Application Security Manager (ASM), Local Traffic Manager (LTM), Access Policy Manager (APM) Apache Hypertext Transfer Protocol (HTTP) server Vulnerability (K40582331)

376863 IBM Hypertext Transfer Protocol (HTTP) Server Multiple Vulnerabilities (6595149)

377911 Oracle Hypertext Transfer Protocol Server (HTTP Server) Multiple Vulnerabilities (CPUJAN2023)

501353 Alpine Linux Security Update for apache2

672022 EulerOS Security Update for httpd (EulerOS-SA-2022-2256)

672041 EulerOS Security Update for httpd (EulerOS-SA-2022-2270)

672052 EulerOS Security Update for httpd (EulerOS-SA-2022-2222)

672060 EulerOS Security Update for httpd (EulerOS-SA-2022-2243)

672082 EulerOS Security Update for httpd (EulerOS-SA-2022-2320)

672128 EulerOS Security Update for httpd (EulerOS-SA-2022-2291)

672228 EulerOS Security Update for httpd (EulerOS-SA-2022-2614)

690877 Free Berkeley Software Distribution (FreeBSD) Security Update for apache httpd (49adfbe5-e7d1-11ec-8fbd-d4c9ef517024)

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

730739 IBM Aspera Faspex Multiple Security Vulnerabilities (6952319)

752247 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2101-1)

752248 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2099-1)

752307 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2302-1)

752326 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2338-1)

752331 SUSE Enterprise Linux Security Update for apache2 (SUSE-SU-2022:2342-1)

940741 AlmaLinux Security Update for httpd:2.4 (ALSA-2022:7647)

940823 AlmaLinux Security Update for httpd (ALSA-2022:8067)

960175 Rocky Linux Security Update for httpd:2.4 (RLSA-2022:7647)

960481 Rocky Linux Security Update for httpd (RLSA-2022:8067)

Exploit/POC from Github

This repository contains a collection of data files on known Common Vulnerabilities and Exposures (CVEs). Each file i…

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Apache	Http Server	All	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Application	Netapp	Clustered Data Ontap	-	All	All	All

cpe:2.3:a:apache:http_server:*:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*:

cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*:

cpe:2.3:a:netapp:clustered_data_ontap:-:*:*:*:*:*:*:*:

Discovery Credit

The Apache HTTP Server project would like to thank Ronald Crane (Zippenhop LLC) for reporting this issue

Social Mentions

Source	Title	Posted (UTC)
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2022-28615 Apache HTTP Server 2.4.53 and earlier may crash or disclose infor… twitter.com/i/web/status/1…	2022-06-08 10:56:00
@ohhara_shiojiri	Apache HTTP Serverの脆弱性情報(Moderate: CVE-2022-26377, Low: CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-29… twitter.com/i/web/status/1…	2022-06-08 14:24:18
@omokazuki	Apache HTTP Serverの脆弱性(Moderate: CVE-2022-26377, Low: CVE-2022-28330, CVE-2022-28614, CVE-2022-28615, CVE-2022-2940… twitter.com/i/web/status/1…	2022-06-08 18:37:00
@CVEreport	CVE-2022-28615 : #Apache HTTP Server 2.4.53 and earlier may crash or disclose information due to a read beyond boun… twitter.com/i/web/status/1…	2022-06-09 16:34:46
/r/netcve	CVE-2022-28615	2022-06-09 16:39:56

← Previous ID

Next ID→