CVE-2021-36160

MITRE | NVD | CVE.ORG | Print: PDF

Summary

CVE	CVE-2021-36160
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	A carefully crafted request uri-path can cause mod_proxy_uwsgi to read above the allocated memory and crash (DoS). This

Risk And Classification

Problem Types: CWE-125

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

References

Reference	Source	Link
September 2021 Apache HTTP Server Vulnerabilities in NetApp Products | NetApp Product Security	CONFIRM	secur
Apache HTTP Server 2.4 vulnerabilities - The Apache HTTP Server Project	MISC	httpd
Apache HTTPD: Multiple Vulnerabilities (GLSA 202208-20) — Gentoo security	GENTOO	secur
[httpd-bugs] 20211005 [Bug 65616] New: CVE-2021-36160 regression		lists.a
[SECURITY] Fedora 35 Update: httpd-2.4.49-1.fc35 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
[httpd-bugs] 20211006 [Bug 65616] CVE-2021-36160 regression		lists.a
Pony Mail!	MLIST	lists.a
Pony Mail!	MLIST	lists.a
[httpd-bugs] 20211012 [Bug 65616] CVE-2021-36160 regression		lists.a
[httpd-users] 20210923 Re: [users@httpd] Re: [External] : [users@httpd] 2.4.49 security fixes: more info		lists.a
[httpd-users] 20210923 [users@httpd] 2.4.49 security fixes: more info		lists.a
[httpd-bugs] 20211005 [Bug 65616] CVE-2021-36160 regression		lists.a
[SECURITY] Fedora 34 Update: httpd-2.4.49-1.fc34 - package-announce - Fedora Mailing-Lists		lists.f
Pony Mail!	MLIST	lists.a
Oracle Critical Patch Update Advisory - April 2022	MISC	www.
Pony Mail!	MLIST	lists.a
Debian -- Security Information -- DSA-4982-1 apache2	DEBIAN	www.
Pony Mail!	MLIST	lists.a
Pony Mail!	MLIST	lists.a
Pony Mail!	MLIST	lists.a
Pony Mail!	MLIST	lists.a
[httpd-cvs] 20210916 [httpd-site] branch main updated: Add descriptions for CVE-2021-33193 CVE-2021-36160		lists.a
[httpd-bugs] 20211008 [Bug 65616] CVE-2021-36160 regression		lists.a
Pony Mail!	MLIST	lists.a
Pony Mail!	MLIST	lists.a
Oracle Critical Patch Update Advisory - January 2022	MISC	www.
Multiple Vulnerabilities in Apache HTTP Server Affecting Cisco Products: November 2021	CISCO	tools.
[SECURITY] [DLA 2768-1] uwsgi security update	MLIST	lists.d
Pony Mail!	MLIST	lists.a

[SECURITY] [DLA 2768-2] uwsgi regression update	MLIST	lists.c
Pony Mail!	MLIST	lists.a
Pony Mail!	MLIST	lists.a
[httpd-bugs] 20211011 [Bug 65616] CVE-2021-36160 regression		lists.a
[httpd-bugs] 20211009 [Bug 65616] CVE-2021-36160 regression		lists.a
[httpd-cvs] 20210916 [httpd-site] branch main updated: Revert "Add descriptions for CVE-2021-33193 CVE-2021-36160"		lists.a
[httpd-users] 20210923 Re: [users@httpd] 2.4.49 security fixes: more info		lists.a
[SECURITY] Fedora 35 Update: httpd-2.4.49-1.fc35 - package-announce - Fedora Mailing-Lists		lists.f
[httpd-users] 20210923 [users@httpd] Re: [External] : [users@httpd] 2.4.49 security fixes: more info		lists.a
[SECURITY] Fedora 34 Update: httpd-2.4.49-1.fc34 - package-announce - Fedora Mailing-Lists	FEDORA	lists.f
CVE Program record	CVE.ORG	www.
NVD vulnerability detail	NVD	nvd.n

Vendor Comments And Credit

Discovery Credit

LEGACY: LI ZHI XIN from NSFocus Security Team

Legacy QID Mappings

- 150401 Apache HTTP Server Out of bounds read - DoS (CVE-2021-36160)
- 159811 Oracle Enterprise Linux Security Update for httpd:2.4 (ELSA-2022-1915)
- 178812 Debian Security Update for uwsgi (DLA 2768-1)
- 178819 Debian Security Update for apache2 (DSA 4982-1)
- 178840 Debian Security Update for uwsgi (DLA 2768-2)
- 182527 Debian Security Update for apache2 (CVE-2021-36160)
- 198516 Ubuntu Security Notification for Apache Hypertext Transfer Protocol (HTTP) Server Vulnerabilities (USN-5090-1)
- 240307 Red Hat Update for httpd:2.4 (RHSA-2022:1915)
- 240698 Red Hat Update for httpd24-httpd (RHSA-2022:6753)
- 240794 Red Hat Update for JBoss Core Services (RHSA-2022:7143)
- 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
- 376961 NetApp Clustered Data Open Network Technology for Appliance Products (ONTAP) Disclosure of Sensitive Information

Vulnerability (NTAP-20211008-0004)

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

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)

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)

730211 Apache Hypertext Transfer Protocol Server (HTTP Server) Denial of Service (DoS) Vulnerability

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)

900387 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (5488)

900966 Common Base Linux Mariner (CBL-Mariner) Security Update for httpd (6485-1)

940509 AlmaLinux Security Update for httpd:2.4 (ALSA-2022:1915)

960327 Rocky Linux Security Update for httpd:2.4 (RLSA-2022:1915)