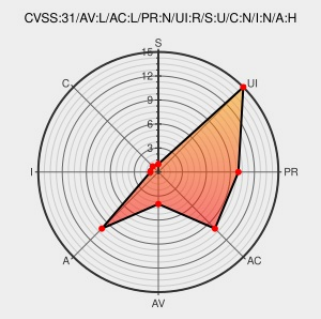
CVE-2021-45958

Published on: Not Yet Published

Last Modified on: 09/10/2022 02:38:00 AM UTC

CVE-2021-45958

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



Certain versions of Debian Linux from Debian contain the following vulnerability:

UltraJSON (aka ujson) through 5.1.0 has a stack-based buffer overflow in Buffer_AppendIndentUnchecked (called from encode). Exploitation can, for example, use a large amount of indentation.

CVE-2021-45958 has been assigned by cve@mitre.org to track the vulnerability - currently rated as MEDIUM severity.

CVSS3 Score: 5.5 - MEDIUM

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

CVSS2 Score: 4.3 - MEDIUM

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

CVE References

Description	Tags	Link
36009 - oss-fuzz - OSS-Fuzz: Fuzzing the planet - Monorail	bugs.chromium.org text/html	MISC bugs.chromium.org/p/oss-fuzz/issues/detail?id=36009
[SECURITY] Fedora 36 Update: python-fastapi-0.75.2-1.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-d1452fd421

[SECURITY] [DLA 2929-1] ujson security update	lists.debian.org text/html	MLIST [debian-lts-announce] 20220226 [SECURITY] [DLA 2929-1] ujson security update
oss-fuzz-vulns/OSV-2021-955.yaml at main · google/oss-fuzz-vulns · GitHub	github.com text/html	MISC github.com/google/oss-fuzz-vulns/blob/main/vulns/ujson/OSV-2021-955.yaml
Fix unchecked buffer overflows (CVE-2021-45958). by bwoodsend · Pull Request #504 · ultrajson/ultrajson · GitHub	github.com text/html	CONFIRM github.com/ultrajson/ultrajson/pull/504
[SECURITY] Fedora 35 Update: python-ujson-5.4.0-1.fc35 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-33e816bc37
[SECURITY] Fedora 36 Update: python-fastapi-0.75.0-3.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-dbf6e00ba8
CVE-2021-45958 from oss-fuzz report · Issue #502 · ultrajson/ultrajson · GitHub	github.com text/html	MISC github.com/ultrajson/ultrajson/issues/502#issuecomment-1031747284
[SECURITY] Fedora 36 Update: python-ujson-5.2.0-1.fc36 - package-announce - Fedora Mailing-Lists	lists.fedoraproject.org text/html	FEDORA FEDORA-2022-569b6b45e2
Segmentation fault with large indent · Issue #501 · ultrajson/ultrajson · GitHub	github.com text/html	MISC github.com/ultrajson/ultrajson/issues/501

Related QID Numbers

179094 Debian Security Update for ujson (DLA 2929-1)

182506 Debian Security Update for ujson (CVE-2021-45958)

283003 Fedora Security Update for python (FEDORA-2022-33e816bc37)

502348 Alpine Linux Security Update for py3-ujson

753979 SUSE Enterprise Linux Security Update for python-ujson (SUSE-SU-2023:2134-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Fedoraproject	Fedora	35	All	All	All
Operating System	Fedoraproject	Fedora	36	All	All	All
Operating System	Fedoraproject	Fedora	37	All	All	All
Application	Ultrajson Project	Ultrajson	All	All	All	All
Application	Ultrajson Project	Ultrajson	All	All	All	All
Application	Ultrajson Project	Ultrajson	All	All	All	All

Application	Ultrajson Project	Ultrajson	All	All	All	All

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*
cpe:2.3:o:fedoraproject:fedora:35:*:*:*:*:*:*:*
cpe:2.3:o:fedoraproject:fedora:36:*:*:*:*:*:*:*
cpe:2.3:o:fedoraproject:fedora:37:*:*:*:*:*:*:*
cpe:2.3:a:ultrajson_project:ultrajson:*:*:*:*:*:python:*:*
cpe:2.3:a:ultrajson_project:ultrajson:*:*:*:*:*:python:*:*
cpe:2.3:a:ultrajson_project:ultrajson:*:*:*:*:*:python:*:*

No vendor comments have been submitted for this CVE

Social Mentions

Source	Title	Posted (UTC)
@CVEreport	CVE-2021-45958 : UltraJSON aka ujson 4.0.2 through 5.0.0 has a stack-based buffer overflow in Buffer_AppendIndent… twitter.com/i/web/status/1…	2022-01-01 00:11:20
@Robo_Alerts	Potentially Critical CVE Detected! CVE-2021-45958 Description: UltraJSON (aka ujson) 4.0.2 through 5.0.0 has a stac… twitter.com/i/web/status/1…	2022-01-01 00:56:27

← Previous ID

Next ID→