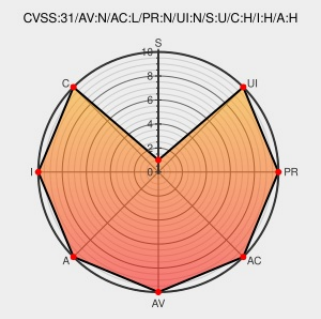
CVE-2019-11834

Published on: 05/09/2019 12:00:00 AM UTC

Last Modified on: 05/03/2022 02:50:00 PM UTC

CVE-2019-11834

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



Certain versions of Cjson from Cjson Project contain the following vulnerability:

cJSON before 1.7.11 allows out-of-bounds access, related to \x00 in a string literal.

CVE-2019-11834 has been assigned by cve@mitre.org to track the vulnerability - currently rated as CRITICAL severity.

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

CVE References

Description	Tags	Link
Release 1.7.11 · DaveGamble/cJSON · GitHub	Release Notes Third Party Advisory github.com text/html	MISC github.com/DaveGamble/cJSON/releases/tag/v1.7.11

cJSON_Minify cross-border read&write 1 · Issue #337 · DaveGamble/cJSON · GitHub	Exploit Third Party Advisory github.com text/html	MISC github.com/DaveGamble/cJSON/issues/337
Oracle Critical Patch Update Advisory - October 2020	www.oracle.com text/html	MISC www.oracle.com/security-alerts/cpuoct2020.html
Comparing c69134d...93688cb · DaveGamble/cJSON · GitHub	Patch Third Party Advisory github.com text/html	MISC github.com/DaveGamble/cJSON/compare/c69134d...93688cb

Related QID Numbers

905174 Common Base Linux Mariner (CBL-Mariner) Security Update for libglvnd (12515)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Cjson Project	Cjson	All	All	All	All
Application	Cjson Project	Cjson	All	All	All	All
Application	Oracle	Timesten In-memory Database	All	All	All	All

cpe:2.3:a:cjson_project:cjson:*:*:*:*:*:*:*:*:

cpe:2.3:a:cjson_project:cjson:*:*:*:*:*:*:*:*:

cpe:2.3:a:oracle:timesten_in-memory_database:*:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→