



CVE-2023-46301

[MITRE](#)[NVD](#)[CVE.ORG](#)[JSON API](#)[Print: PDF](#)

Summary

CVE	CVE-2023-46301
State	PUBLIC
Assigner	cve@mitre.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-10-22 04:15:00 UTC
Updated	2023-10-31 17:08:00 UTC
Description	iTerm2 before 3.4.20 allow (potentially remote) code execution because of mishandling of certain escape sequences relate

Risk And Classification

Problem Types: CWE-116

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Item2	Item2	All	All	All	All

References

Reference	Source	Link	Tags
iTerm2 - macOS Terminal Replacement	MISC	item2.com	
Fixes for method 1. · gnachman/iTerm2@b2268b0 · GitHub	MISC	github.com	
From Terminal Output to Arbitrary Remote Code Execution solid-snail blog	MISC	blog.solidsnail.com	
Fix ReportUpload vulnerability · gnachman/iTerm2@85cbf5e · GitHub	MISC	github.com	
CVE Program record	CVE.ORG	www.cve.org	canonical
NVD vulnerability detail	NVD	nvd.nist.gov	canonical, analysis

No vendor comments have been submitted for this CVE.

There are currently no legacy QID mappings associated with this CVE.

completeness or usefulness of any information, opinion, advice or other content. EACH USER WILL BE SOLELY RESPONSIBLE FOR ANY consequences of his or her direct or indirect use of this web site. ALL WARRANTIES OF ANY KIND ARE EXPRESSLY DISCLAIMED. This site will NOT BE LIABLE FOR ANY DIRECT, INDIRECT or any other kind of loss.

CVE, CWE, and OVAL are registered trademarks of [The MITRE Corporation](#) and the authoritative source of CVE content is [MITRE's CVE web site](#). This site includes MITRE data granted under the following [license](#).

Free CVE JSON API cve.report/api

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