



CVE-2021-41253

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

Summary

CVE	CVE-2021-41253
State	PUBLIC
Assigner	security-advisories@github.com
Source Priority	CVE Program / NVD first with legacy fallback
Published	2021-11-08 22:15:00 UTC
Updated	2022-10-24 16:07:00 UTC
Description	Zydis is an x86/x86-64 disassembler library. Users of Zydis versions v3.2.0 and older that use the string functions provided

Risk And Classification

Problem Types: CWE-908

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Zyantific	Zydis	All	All	All	All

References

Reference	Source	Link
huntr: Disclose & Fix Security Vulnerabilities in Open Source	MISC	huntr.d
Possible heap buffer overflow when using zycore string functions in formatter hooks · Advisory · zyantific/zydis · GitHub	CONFIRM	github.
huntr: Disclose & Fix Security Vulnerabilities in Open Source	MISC	huntr.d
Fix struct initialization in formatter · zyantific/zydis@55dd08c · GitHub	MISC	github.
CVE Program record	CVE.ORG	www.c
NVD vulnerability detail	NVD	nvd.nis

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

[184630](#) Debian Security Update for zydis (CVE-2021-41253)

[690953](#) Free Berkeley Software Distribution (FreeBSD) Security Update for zydis (d487d4fc-43a8-11ed-8b01-b42e991fc52e)

© [CVE.report](#) 2026 |

Use of this information constitutes acceptance for use in an AS IS condition. There are NO warranties, implied or otherwise, with regard to this information or its use. Any use of this information is at the user's risk. It is the responsibility of user to evaluate the accuracy, 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](#)