



CVE-2021-33641

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

Summary

CVE	CVE-2021-33641
State	PUBLIC
Assigner	securities@openeuler.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2023-01-20 21:15:00 UTC
Updated	2023-09-26 19:53:00 UTC
Description	When processing files, malloc stores the data of the current line. When processing comments, malloc incorrectly accesses

Risk And Classification

Problem Types: CWE-416

NVD Known Affected Configurations (CPE 2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Application	Openeuler	Byacc	All	All	All	All

References

Reference	Source	Link	Tags
Login - Gitee.com	MISC	gitee.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.

Legacy QID Mappings

[355423](#) Amazon Linux Security Advisory for byacc : ALAS2023-2023-204

[672725](#) EulerOS Security Update for byacc (EulerOS-SA-2023-1436)

[672754](#) EulerOS Security Update for byacc (EulerOS-SA-2023-1461)

[672814](#) EulerOS Security Update for byacc (EulerOS-SA-2023-1520)

[672821](#) EulerOS Security Update for byacc (EulerOS-SA-2023-1545)

672917 EulerOS Security Update for byacc (EulerOS-SA-2023-1778)

672931 EulerOS Security Update for byacc (EulerOS-SA-2023-1756)

© [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](#)