



CVE-2015-4054

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

Summary

CVE	CVE-2015-4054
State	PUBLIC
Assigner	security@debian.org
Source Priority	CVE Program / NVD first with legacy fallback
Published	2017-05-23 04:29:00 UTC
Updated	2020-11-03 18:16:00 UTC
Description	PgBouncer before 1.5.5 allows remote attackers to cause a denial of service (NULL pointer dereference and crash) by send

Risk And Classification

Problem Types: CWE-476

NVD Known Affected Configurations (CPE 2.3)

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

References

Reference	Source	Link
oss-security - Re: CVE Request: pgbouncer: DoS/remote crash: invalid packet order causes lookup of NULL pointer	MLIST	www.oper
Check if auth_user is set. · pgbouncer/pgbouncer@74d6e5f · GitHub	CONFIRM	github.cor
Check if auth_user is set. · pgbouncer/pgbouncer@edab5be · GitHub	CONFIRM	github.cor
PgBouncer src/client.c' Denial of Service Vulnerability	BID	www.secu
pgbouncer 1.5.4 segmentation fault · Issue #42 · pgbouncer/pgbouncer · GitHub	CONFIRM	github.cor
PgBouncer changelog	CONFIRM	pgbounc
PgBouncer: Multiple vulnerabilities (GLSA 201701-24) — Gentoo security	GENTOO	security.g
CVE Program record	CVE.ORG	www.cve.
NVD vulnerability detail	NVD	nvd.nist.g

No vendor comments have been submitted for this CVE.

Legacy QID Mappings

© [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](#).

CVE.report and Source URL Uptime Status [status.cve.report](#)