

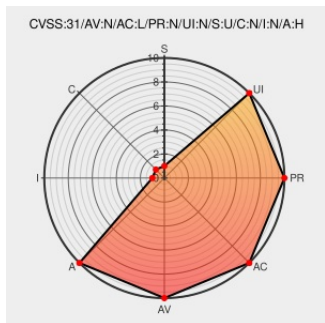


CVE-2017-18359

Published on: 01/25/2019 12:00:00 AM UTC

Last Modified on: 04/06/2022 06:33:00 PM UTC

CVE-2017-18359

[Source: Mitre](#)[Source: NIST](#)[CVE.ORG](#)[Print: PDF](#) 

Certain versions of [Debian Linux](#) from [Debian](#) contain the following vulnerability:

PostGIS 2.x before 2.3.3, as used with PostgreSQL, allows remote attackers to cause a denial of service via crafted ST_AsX3D function input, as demonstrated by an abnormal server termination for "SELECT ST_AsX3D('LINESTRING EMPTY');" because empty geometries are mishandled.

CVE-2017-18359 has been assigned by [M](#) cve@mitre.org to track the vulnerability - currently rated as **HIGH** severity.

CVSS3 Score: **7.5 - HIGH**

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

CVSS2 Score: **5 - MEDIUM**

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

CVE References

Description	Tags	Link
[SECURITY] [DLA 1653-1] postgres security update	Third Party Advisory lists.debian.org text/html	MLIST [debian-lts-announce] 20190131 [SECURITY] [DLA 1653-1] postgres security update

Changeset 15444 – PostGIS	Patch Third Party Advisory trac.osgeo.org text/html	 MISC trac.osgeo.org/postgis/changeset/15444
[SECURITY] [DLA 2857-1] postgres security update	lists.debian.org text/html	 MLIST [debian-lts-announce] 20211227 [SECURITY] [DLA 2857-1] postgres security update
#3704 (ST_AsX3D returns random data / crashes client) – PostGIS	Third Party Advisory trac.osgeo.org text/html	 MISC trac.osgeo.org/postgis/ticket/3704
Changeset 15445 – PostGIS	Patch Third Party Advisory trac.osgeo.org text/html	 MISC trac.osgeo.org/postgis/changeset/15445

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

Related QID Numbers

[178963](#) Debian Security Update for postgres (DLA 2857-1)

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Application	Postgis	Postgis	All	All	All	All
Application	Postgis	Postgis	All	All	All	All
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:						
cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:						
cpe:2.3:a:postgis:postgis:*:*:*:*:postgresql:*:*:						
cpe:2.3:a:postgis:postgis:*:*:*:*:postgresql:*:*:						

No vendor comments have been submitted for this CVE

© [CVE.report](#) 2023   |

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](#)