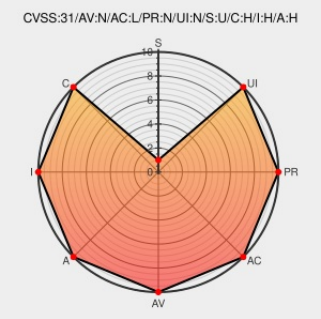
CVE-2015-3166

Published on: 11/20/2019 12:00:00 AM UTC

Last Modified on: 03/23/2021 11:26:08 PM UTC

CVE-2015-3166

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF



Certain versions of Ubuntu Linux from Canonical contain the following vulnerability:

The snprintf implementation in PostgreSQL before 9.0.20, 9.1.x before 9.1.16, 9.2.x before 9.2.11, 9.3.x before 9.3.7, and 9.4.x before 9.4.2 does not properly handle system-call errors, which allows attackers to obtain sensitive information or have other unspecified impact via unknown vectors, as demonstrated by an out-of-memory error.

CVE-2015-3166 has been assigned by secalert@redhat.com to track the vulnerability - currently rated as CRITICAL severity.

Affected Vendor/Software: **PostgreSQL Global Development Group** - **PostgreSQL** version **before 9.0.20**

Affected Vendor/Software: **PostgreSQL Global Development Group** - **PostgreSQL** version **9.1.x before 9.1.16**

Affected Vendor/Software: **PostgreSQL Global Development Group** - **PostgreSQL** version **9.2.x before 9.2.11**

Affected Vendor/Software: **PostgreSQL Global Development Group** - **PostgreSQL** version **9.3.x before 9.3.7**

Affected Vendor/Software: **PostgreSQL Global Development Group** - **PostgreSQL** version **and 9.4.x before 9.4.2**

CVSS3 Score: 9.8 - CRITICAL

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

CVSS2 Score: 7.5 - HIGH

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

Impact	Impact	Impact
PARTIAL	PARTIAL	PARTIAL

CVE References

Description	Tags	Link
PostgreSQL: Documentation: 9.3: Release 9.3.7	Release Notes, Vendor Advisory, www.postgresql.org, text/html	MISC www.postgresql.org/docs/9.3/static/release-9-3-7.html
Debian -- Security Information -- DSA-3269-1 postgresql-9.1	Third Party Advisory, www.debian.org, Depreciated Link, text/html	MISC www.debian.org/security/2015/dsa-3269
Debian -- Security Information -- DSA-3270-1 postgresql-9.4	Third Party Advisory, www.debian.org, Depreciated Link, text/html	MISC www.debian.org/security/2015/dsa-3270
USN-2621-1: PostgreSQL vulnerabilities | Ubuntu	Third Party Advisory, ubuntu.com, text/html	MISC ubuntu.com/usn/usn-2621-1
PostgreSQL: Documentation: 9.4: Release 9.4.2	Release Notes, Vendor Advisory, www.postgresql.org, text/html	MISC www.postgresql.org/docs/9.4/static/release-9-4-2.html
PostgreSQL: Documentation: 9.2: Release 9.2.11	Release Notes, Vendor Advisory, www.postgresql.org, text/html	MISC www.postgresql.org/docs/9.2/static/release-9-2-11.html
PostgreSQL: Documentation: 9.0: Release 9.0.20	Release Notes, Vendor Advisory, www.postgresql.org, text/html	MISC www.postgresql.org/docs/9.0/static/release-9-0-20.html
PostgreSQL: PostgreSQL 9.4.2, 9.3.7, 9.2.11, 9.1.16, and 9.0.20 released!	Vendor Advisory, www.postgresql.org, text/html	MISC www.postgresql.org/about/news/1587/
PostgreSQL: Documentation: 9.1: Release 9.1.16	Release Notes, Vendor Advisory, www.postgresql.org, text/html	MISC www.postgresql.org/docs/9.1/static/release-9-1-16.html

There are currently no QIDs associated with this CVE

Known Affected Configurations (CPE V2.3)

Type	Vendor	Product	Version	Update	Edition	Language
Operating	Canonical	Ubuntu Linux	12.04	All	All	All

System						
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Canonical	Ubuntu Linux	12.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.04	All	All	All
Operating System	Canonical	Ubuntu Linux	14.10	All	All	All
Operating System	Canonical	Ubuntu Linux	15.04	All	All	All
Operating System	Debian	Debian Linux	7.0	All	All	All
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	7.0	All	All	All
Operating System	Debian	Debian Linux	8.0	All	All	All
Operating System	Debian	Debian Linux	9.0	All	All	All
Application	Postgresql	Postgresql	All	All	All	All
Application	Postgresql	Postgresql	All	All	All	All

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:12.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.04:*:*:*:lts:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:14.10:*:*:*:*:*:*:*:

cpe:2.3:o:canonical:ubuntu_linux:15.04:*:*:*:*:*:*:*:

cpe:2.3:o:debian:debian_linux:7.0:*:*:*:*:*:*:*:

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:7.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:8.0:*:*:*:*:*:*:*

cpe:2.3:o:debian:debian_linux:9.0:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:*:*:*:*:*:*:*:*

cpe:2.3:a:postgresql:postgresql:*:*:*:*:*:*:*:*

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→