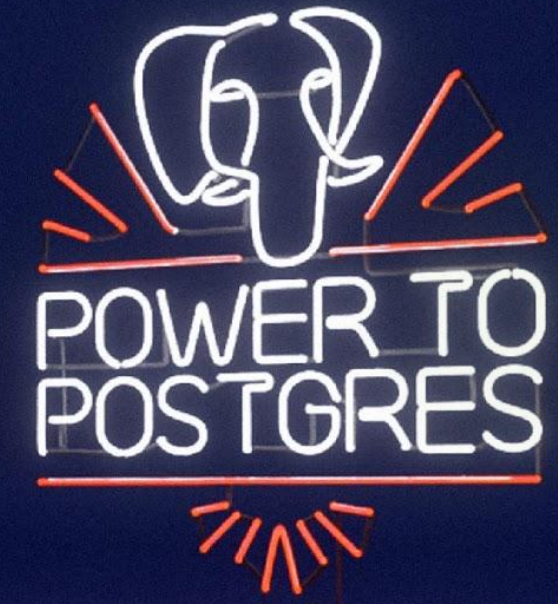
15 Nov 2021

MITM21 Vulnerability



Simon Riggs
Postgres Fellow

EDB

Update your servers

- New Security & Maintenance release of PostgreSQL and EPAS is available
- **Recently reported issue of MITM21 has been fixed!**
- Please update very soon to these latest releases
  - 14.1
  - 13.5
  - 12.9
  - 11.14
  - 10.17
  - 9.6.24

- The rest of this webinar is about the security fixes in this release

What just happened?

New vulnerability has been discovered on PostgreSQL

- When we communicate client -> server, requesting an SSL connection, all of the the response bytes are buffered
- If more bytes are sent then just the response byte, the remaining bytes aren't **flushed** as they should have been
- So when we begin an encrypted conversation we start with a buffer full of messages to process...

How can this vulnerability be exploited?

- A type of attack known as a Man In The Middle (MITM) attack can use this vulnerability to inject additional messages into the communication between client and server. Hence why we call this issue **MITM21**.

Is this a new kind of attack?

- No, it is a known vulnerability pattern in other software
  - CVE-2011-0411 affecting mailserver "Postfix"
- Allows a "plaintext command injection" exploit

- In most cases network staff will be well aware of protections
- If all of your network is safe

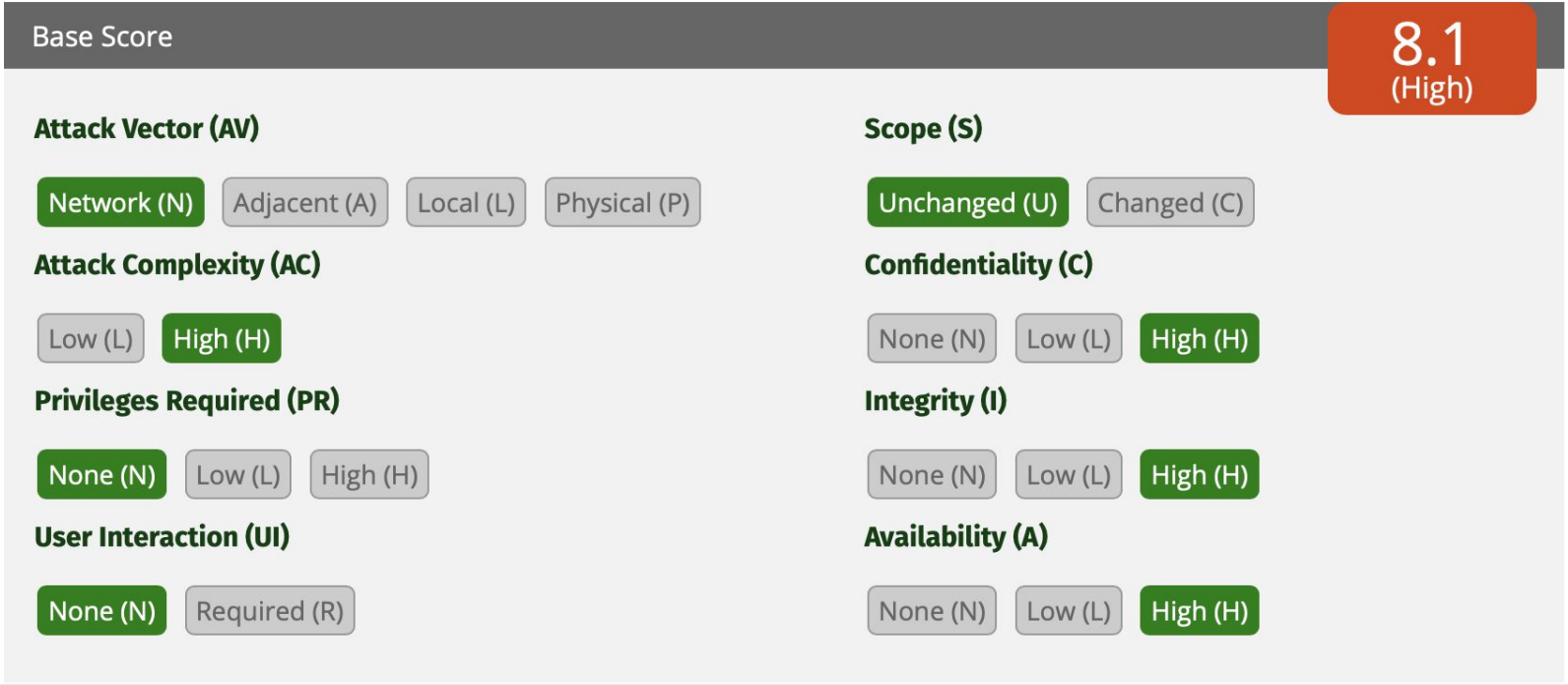
What is the impact?

Plaintext command injection (CVE-2021-23214)

- Can be used by a MITM to inject additional commands to the **server**
- Not very useful, unless the server doesn't demand authentication data, hence why this is only a risk in these cases (SQL works on PG10+)

```
SELECT * FROM pg_hba_file_rules
WHERE (auth_method = 'cert' or
        (auth_method = 'trust' and options::text like '%clientcert%'))
and type like 'host%' and error is null;
```

CVSSv3 Rating: CVE-2021-23214 (Server)

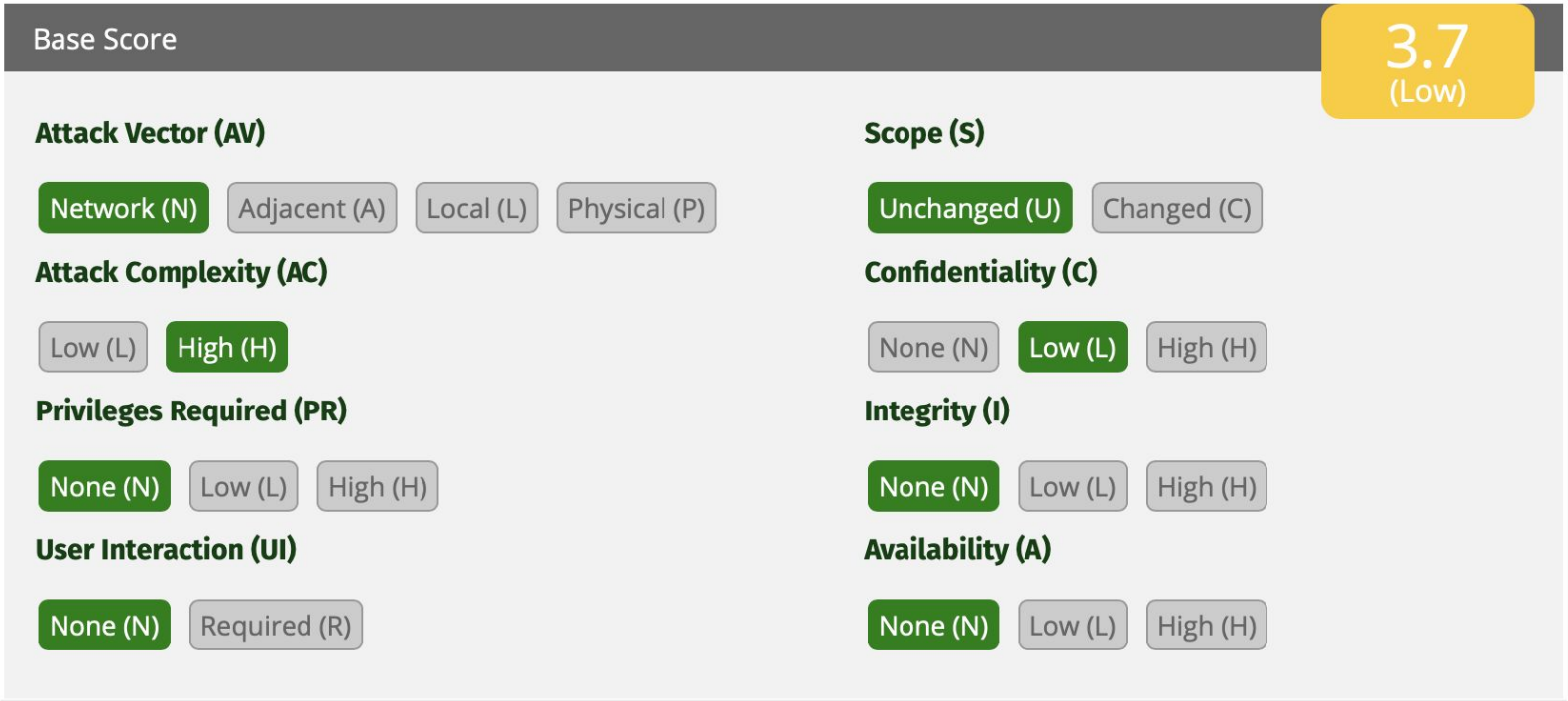


Plaintext command injection (CVE-2021-23222)

- Can be used by a MITM to inject responses to the **client**
- No exploit is known, except when CVE-2021-23214 is unpatched, an attacker with other credentials might be able to trick you into revealing high value information, such as passwords (if any are used in the exchange)
- So you ***might*** be safe

- There is no safe way to know whether CVE-2021-23214 is patched, since if you ask the server, the MITM could lie…

CVSSv3 Rating: CVE-2021-23222 (Client)



Two pieces of software = Two CVEs

- CVE-2021-23214 for PostgreSQL Server
- CVE-2021-23222 for PostgreSQL Client
- Most other software has NOT filed separate CVE numbers, they just refer to the same two vulnerabilities
- Be careful, because patching just those 2 items may not be enough

What to update?

Upgrade your servers

- Upgrade any server at Major Release 9.6 or earlier
  - 9.6 upgrade to a later major release, possibly using pglogical2
  - 9.5 upgrade to a later major release, possibly using pglogical2
  - 9.4 upgrade to a later major release, possibly using pglogical2
  - or earlier upgrade to a later major release
- Remember to update all related servers: standbys, PEM server etc..
- If you have difficulty upgrading
  - Use pglogical2, if possible (requires 9.4 or later as source)
  - Consider using BDR to make all later upgrading easier

Update your servers

- If you are on PostgreSQL 10 or later, update to the latest releases
  - 14.1 PostgreSQL only
  - 13.5 PostgreSQL, EPAS and EPX
  - 12.9 PostgreSQL, EPAS and EPX
  - 11.14 PostgreSQL, EPAS and EPX
  - 10.17 PostgreSQL, EPAS and EPX
  - 9.6.24 PostgreSQL, EPAS and EPX

- Earlier versions are likely to be vulnerable also since the affected code has not changed in some years

Update your session poolers

- PGBouncer, Pgpool and Odyssey are all affected by one or both CVEs
- Update to the latest release
  - PGBouncer 1.16.1+ 12 Nov EDB
  - Odyssey 1.2 12 Nov
  - Pgpool 18 Nov

Update your MacOS/Windows installers

- EDB One-Click installers, on Download page from postgresql.org
  - These contain both Client and Server software
  - New versions are already available
  - https://www.enterprisedb.com/downloads/postgres-postgresql-downloads

- If you have installed them on your laptop and then use them to access PostgreSQL servers then these need to be updated

- If you have pgAdmin installer, then download and upgrade also (this week)

Update (some of) your clients

- These types of client are already **known safe** from CVE-2021-23222
  - jdbc (java)
  - npgsql (.NET)
  - node-postgres (node.js)
  - rust-postgres (rust)
  - pgx (Go)
  - epgsql (Erlang)

- These clients are known to be affected by CVE-2021-23222
  - libpq
  - PostgresClientKit (swift)

Update your clients

- libpq is a client library for PostgreSQL
- Typically, this will be dynamically linked by applications and drivers
- These drivers are known to use libpq, so require upgrading
  - ODBC
  - psycopg2 (Python)
  - DBD::Pg (perl)
  - php-pgsql (PHP)
  - ruby-pg (Ruby)
  - pgtclng (Tcl)
  - RPostgreSQL (R)
  - HDBC (Haskell)

Update your EDB clients

- EDB software with security updates
  - ODBC 13.01.0000.01 12 Nov
  - OCL 13.1..4.2-2 12 Nov
  - Replication Server 6.2.15-2 12 Nov
  - PEM 8.2.0-10, 7.16.1-2 12 Nov

Statically linked clients

- Some people compile their own client code, and in some cases link libraries statically, though this is not common
  - In that case, you will need to rebuild your binary with the upgraded library

Upgrade your Cloud DBaaS

BIGANIMAL

- BigAnimal 13.5 upgrading today, 16 Nov

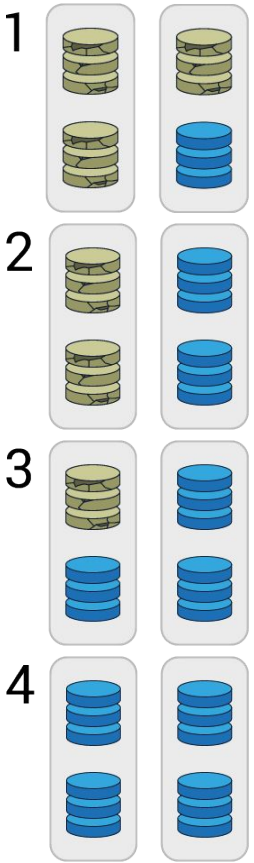
- AWS RDS 13.4 awaiting upgrade
- Azure Uncertain
- Google 13.4 needs upgrade, upgraded to 13.4 on 29 Oct, ~10 weeks behind

Upgrading

BDR Rolling System Upgrades

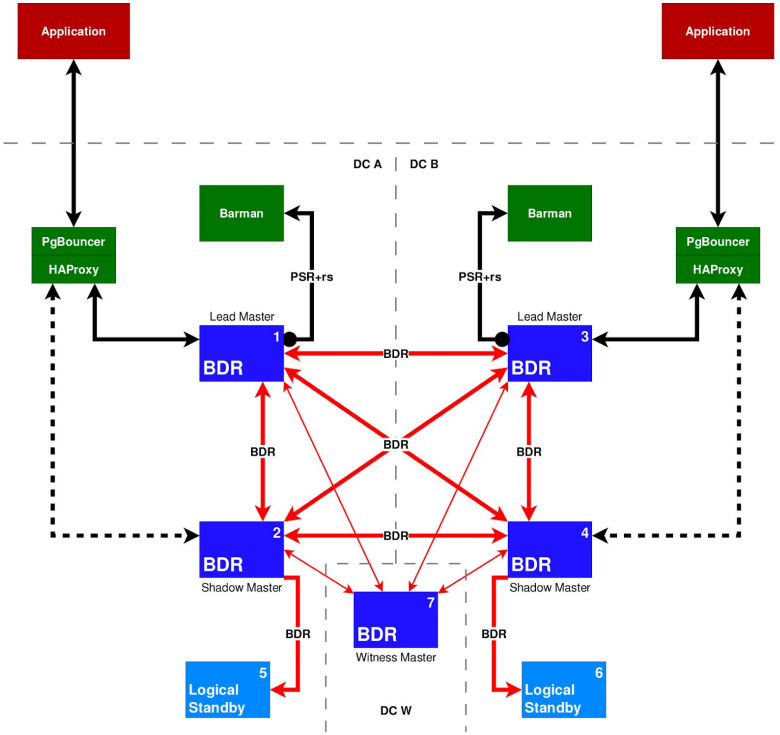
- Automatic Rolling System Upgrades
  - Works across major software releases of OS, Database server and Postgres-BDR
  - Can be manually controlled, if desired
  - Inter-node protocols are re-negotiated for each link, all protocols backwards compatible

- Resolves the largest source of downtime
  - Security/Maintenance releases - 4 times per year
  - Unscheduled bugs ~1 per year
  - Parameter changes, hardware changes also



Very High Availability with Postgres-BDR

- Multi-Master/Active-Active
- Multiple Data Centres (DCs)
- Application access to Lead Node, fast failover to Shadow Node for **99.999% Availability**
- Tolerant of down nodes, automatically recovers from node outage and network partition
- [Kubernetes: Self-healing]



Thanks!

simon.riggs@enterprisedb.com

EDB