



EDB POSTGRES® AI · MIGRATIONS

Greenplum® after May 2024: A patch governance brief

What the move to a closed-source release model changed for the open-source line, what it did not change, and the questions your security and compliance teams will ask.

OSS supply chain · CVE response · PCI DSS v4.0.1 Requirements 6.3.3 and 12.3.4

A licensing change with an operational tail

For any Greenplum deployment, the control question is who issues security fixes, on what timeline, and whether you can show it.

Most of the discussion about Greenplum going closed source has been commercial: pricing, lock-in, roadmap. That framing rarely moves a security or compliance stakeholder, because none of it is a control question.

There is a control question underneath it, and it is narrower and more answerable than the commercial one: for any given Greenplum deployment, who issues security fixes, on what timeline, and can you show it? This brief translates the May 2024 change into the language those teams already use.

The answer depends on which deployment you run. A current commercial Tanzu Greenplum subscription is a supported product. The archived open-source line, and forks your own team supports, are where PCI DSS Requirements 12.3.4 and 6.3.3 become a resourcing question. Section 05 sets out a test to apply to any provider, EDB included.

2024

May: Greenplum moves to a closed-source release model; public repositories archived read-only

12

Months: PCI DSS v4.0.1 technology review cycle, Requirement 12.3.4

1

Month: PCI DSS v4.0.1 window to install critical security patches, Requirement 6.3.3

Sources: Broadcom's public Greenplum repositories (github.com/greenplum-db/gpdb-archive, archived read-only, last updated May 2024) and release communications; PCI Security Standards Council, PCI DSS v4.0.1, Requirements 12.3.4 and 6.3.3.



The facts, dated

Four owners since 2010, and one change to the release model.

WHEN	WHAT HAPPENED
2010 to 2019	EMC acquires Greenplum in 2010. Greenplum moves to Pivotal in 2012, and VMware acquires Pivotal in 2019.
September 2023	Greenplum 7.0.0 released: the last major release of the open-source line.
November 2023	Broadcom completes its acquisition of VMware, bringing Greenplum into the Tanzu portfolio.
May 2024	Tanzu by Broadcom moves future Greenplum releases to a closed-source model inside its commercial suite. The public Greenplum repositories are archived and made read-only.

Source: ownership history and the May 2024 change are matters of public record, per Broadcom's own repositories, release history and product communications.

This is not an end-of-life notice

Greenplum has no publicly published end-of-life date, and this brief does not assert one.

If you hold a current commercial Tanzu Greenplum subscription, you have a supported product with a vendor issuing fixes, and the review in section 04 already has its answer.

The governance question applies to two narrower situations: deployments running the archived open-source line with no commercial subscription, and deployments running a community fork.



Which situation are you in?

Four deployment situations, and four different answers to who issues the fixes.

DEPLOYMENT	WHO ISSUES SECURITY FIXES	GOVERNANCE POSITION
Commercial Tanzu Greenplum subscription	Broadcom, under your subscription terms	Supported product. The section 04 review has a ready answer. Confirm your entitlement covers the versions you run, and check any per-version lifecycle dates Broadcom publishes to entitled customers in its support portal.
Archived open-source Greenplum, no subscription	Nobody, by default	The repositories are read-only. There is no upstream issuing fixes for this line. This is the situation section 04 addresses.
A community fork (for example, Apache Cloudberry)	The community, on a best-efforts basis	A legitimate choice with a real obligation attached: somebody owns CVE triage, patching and packaging, and if that somebody is your team, that is a resourced role, not a background task.
A vendor-supported fork	That vendor, under contract	Supported. Ask the section 05 questions of any vendor, including EDB, rather than accepting the claim.

Situations as of October 2026. Greenplum has no publicly published end-of-life date, and this table does not assert one.

Read this before taking section 04 to your auditor

Anyone telling you the compliance argument applies to Greenplum generally is overstating it, and your QSA will notice.

The obligation follows the deployment, not the product name: classify each cluster on its own, since many estates are in more than one situation.

Where a cluster's answer is "nobody, by default," take that finding into section 04 and, if one is needed, into the remediation plan.

What the standard actually requires

This section applies only where the Greenplum environment stores, processes, or transmits cardholder data. Confirm scope with your QSA before assuming it applies.

1

Requirement 12.3.4: annual review

At least once every 12 months, review the hardware and software technologies in use, including whether each still receives security fixes from its vendor promptly. Document a remediation plan, approved by senior management, for outdated technologies, including any whose vendor has announced end-of-life plans. Mandatory since March 31, 2025.

2

Requirement 6.3.3: patch timeline

Patches for critical vulnerabilities must be installed within one month of release. The requirement assumes a patch exists. Where no upstream is issuing patches, waiting cannot satisfy it: someone else has to produce the patch, or you document a compensating control your assessor accepts. That is the whole practical question: who, and how fast.

What this means for the archived open-source line

Greenplum has no announced end-of-life, so this brief's argument does not rest on that part of 12.3.4. It rests on the review's first question. On the archived open-source line with no subscription, the honest answer is that no vendor issues security fixes for it, and your QSA may treat it as outdated technology that needs an approved plan. That determination is your assessor's, not this brief's.

Under SOX Section 404 there is no bright-line software rule. Patch management, including whether software is vendor-supported, is a standard IT general controls area: an audit conversation, not an automatic finding.

Sources: PCI Security Standards Council, PCI DSS v4.0.1, Requirements 12.3.4 and 6.3.3. PCI DSS v4.0 was retired on December 31, 2024. Sarbanes-Oxley Act of 2002, Section 404.

The honest framing

Neither requirement names Greenplum, Broadcom, or any product, and neither is triggered by a license change as such. What 12.3.4 asks is whether a vendor still issues security fixes for the component you run.

The remediation plan it requires is platform-neutral: it does not have to name EDB, or anyone.



A fair test, applied to everyone

If you move to a supported fork, from EDB or anyone else, these are the questions that turn “supported” from a claim into an entitlement. Ask all of them, of every candidate, including EDB.

CVE response

What is the committed timeline from a CVE being published to a patched package being available to you? Is that in the contract or in a blog post?

Package integrity

Are packages signed? How is the signing key managed, and how do you verify a package before installation?

Bill of materials

Can the provider supply an SBOM for the distribution, and keep it current as components change?

Backport policy

When a fix lands upstream in a newer line, is it backported to the version you run, and for how long?

Version support window

How long is your current major version supported, and is that published or negotiated per customer?

Provenance

Which upstream does the fork track, how are changes brought across, and what happens if that upstream stops moving?

Evidence on demand

Can the provider produce, for an auditor, a record of which fixes were applied to your deployment and when?

This is the one most often assumed and least often available.

It is also the kind of record an assessor reviews when testing Requirement 6.3.3: installed patches compared against the vendor’s latest security patch information.



What EDB offers against that list

Ask EDB for the section 05 answers in writing, as you would of anyone.

An Apache-licensed fork, publicly developed

EDB Postgres® AI for WarehousePG is an Apache-licensed fork of the last open-source Greenplum release, developed in public on GitHub. The property that made Greenplum a defensible choice originally is the property this restores.

Supported, with CVE patching and signed packages

With an EDB subscription: 24x7 break/fix support, CVE remediation and proactive patching, and signed packages delivered through a dedicated EDB repository. These are the specific obligations a team inherits when it self-supports a fork.

A migration path that does not rewrite your estate

WarehousePG is binary compatible with Greenplum 6.x and 7.x, so the remediation plan 12.3.4 asks for does not have to be a multi-year replatforming program. The technical companion, Greenplum to WarehousePG: A technical playbook, covers the mechanism, the version scope, and its limits.

One thing to keep straight

Migrating is not the only compliant answer. A current commercial Tanzu subscription answers 12.3.4 perfectly well, and so does a well-resourced internal team with a documented patch process on a community fork.

What the requirement asks for is a defensible answer and a documented plan, not a particular vendor. Any brief that tells you otherwise is selling rather than advising.

SOURCE LINE	PUBLISHED COMPATIBILITY	FOR THE REMEDIATION PLAN
Greenplum 7.x	Binary compatible	Inside the documented scope.
Greenplum 6.x	Binary compatible	Inside the documented scope; WarehousePG 6 packages are available.
Apache Cloudberry and other forks	No published compatibility claim	Assess separately before it goes into a plan.
Greenplum 4.x and 5.x	No published compatibility claim	Outside the documented scope.

Sources: EDB Postgres AI for WarehousePG documentation (enterprisedb.com/docs/warehousepg/latest); EDB Postgres AI support for Greenplum workloads, documentation and product page (enterprisedb.com/products/support-for-greenplum-workloads).

Four steps, in order

1

Establish which situation you are in

Use the table in section 03: commercial subscription, archived open-source line, community fork, or vendor-supported fork. Most organizations with more than one cluster find they are in more than one situation.

2

Confirm scope with compliance

Check whether any of these environments fall in PCI DSS scope, or support a financial-reporting system subject to ITGC review. This determines whether section 04 applies at all.

3

Start the remediation plan if it applies

12.3.4 requires senior-management approval regardless of which target platform is eventually chosen, so this step is not vendor-specific and does not need to wait on a procurement decision.

4

Ask the section 05 questions

Of every candidate, including EDB. A provider that answers in writing is giving you audit evidence; one that answers verbally is giving you a sales call.

Request an assessment

Request a migration assessment, or contact your EDB account team. If you received this document from an EDB representative, reply to them directly.

enterprisedb.com/contact

Sources

- Greenplum ownership history and the May 2024 move to a closed-source release model, including the archiving of public repositories: matters of public record, per Broadcom's own repositories (github.com/greenplum-db/gpdb-archive), release history and product communications. Greenplum 7.0.0 released September 2023.
- PCI Security Standards Council, PCI DSS v4.0.1, Requirements 12.3.4 and 6.3.3; Requirement 12.3.4 mandatory since March 31, 2025; v4.0 retired December 31, 2024.
- Sarbanes-Oxley Act of 2002, Section 404, and standard IT general controls (ITGC) audit practice.
- EDB Postgres AI for WarehousePG documentation: license, lineage, binary compatibility scope and release notes (enterprisedb.com/docs/warehousepg/latest).
- EDB Postgres AI support for Greenplum workloads: support entitlements, software updates and repository delivery (enterprisedb.com/docs/supported-open-source/warehousepg/edbpggpgsupp); 24x7 break/fix, CVE remediation and signed packages (enterprisedb.com/products/support-for-greenplum-workloads).
- Apache Cloudberry (Incubating): Apache Software Foundation podling, Apache License 2.0.



Know who issues the fixes, and be able to show it.

Greenplum has no published end-of-life date.

What changed in May 2024 is who issues fixes for the open-source line, and the answer belongs in writing before your next annual technology review.

This brief is provided for informational and planning purposes only and does not constitute legal, audit, or compliance advice. EDB is not a law firm, auditor, or Qualified Security Assessor. Consult your own compliance, legal, and QSA advisors to determine how PCI DSS, SOX, or any other regulatory framework applies to your specific environment. Nothing in this document asserts that Greenplum is end-of-life or unsupported; commercially subscribed Tanzu Greenplum deployments are supported by Broadcom. Greenplum® is a registered trademark, and Tanzu a trademark, of Broadcom Inc. and/or its subsidiaries. EDB and EDB Postgres AI are not affiliated with, endorsed by, or sponsored by Broadcom Inc. Any references to Greenplum are for comparative, educational, and interoperability purposes only. PCI DSS is a trademark of PCI Security Standards Council, LLC. Apache, Apache Cloudberry and the Apache feather logo are trademarks of The Apache Software Foundation. Postgres and PostgreSQL are registered trademarks of the PostgreSQL Community Association of Canada and used with their permission. EDB Postgres® AI is a trademark of EnterpriseDB Corporation. © EnterpriseDB Corporation 2026. All rights reserved.

EDB Postgres® AI is the first open, enterprise-grade sovereign data and AI platform, with a secure, compliant, and fully scalable environment, on premises and across clouds. Supported by a global partner network, EDB Postgres AI unifies transactional, analytical, and AI workloads, enabling organizations to operationalize their data and LLMs where, when, and how they need them. For more information, visit enterprisedb.com.

