

## Security Bulletin

# Multiple vulnerabilities in PostgreSQL

Author(s)	:	Eviden PSIRT
Reference	:	PSIRT-5233
Created	:	23 December 2025
Version	:	2.1
Status	:	Remediation
TLP Classification	:	CLEAR
Document date	:	16 January 2026
Keywords	:	CVE-2025-8713 CVE-2025-8714 CVE-8715

**TLP:CLEAR**

*Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.*

**FOR PUBLIC USE**

## List of changes

Version	Date	Description
2.1	2026/01/16	Initial Eviden version

## Executive summary

Multiple vulnerabilities have been discovered in PostgreSQL that could allow an attacker to cause remote code execution and data confidentiality. PostgreSQL optimizer statistics allow a user to read sampled data within a view that the user cannot access. Separately, statistics allow a user to read sampled data that a row security policy intended to hide. PostgreSQL maintains statistics for tables by sampling data available in columns; this data is consulted during the query planning process. Prior to this release, a user could craft a leaky operator that bypassed view access control lists (ACLs) and bypassed row security policies in partitioning or table inheritance hierarchies. Reachable statistics data notably included histograms and most-common-values lists.

### [CVE-2025-8713](#)

PostgreSQL optimizer statistics allow a user to read sampled data within a view that the user cannot access. Separately, statistics allow a user to read sampled data that a row security policy intended to hide. PostgreSQL maintains statistics for tables by sampling data available in columns; this data is consulted during the query planning process. Prior to this release, a user could craft a leaky operator that bypassed view access control lists (ACLs) and bypassed row security policies in partitioning or table inheritance hierarchies. Reachable statistics data notably included histograms and most-common-values lists. CVE-2017-7484 and CVE-2019-10130 intended to close this class of vulnerability, but this gap remained. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected.

### [CVE-2025-8714](#)

Untrusted data inclusion in pg\_dump in PostgreSQL allows a malicious superuser of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql meta-commands. pg\_dumpall is also affected. pg\_restore is affected when used to generate a plain-format dump. This is similar to MySQL CVE-2024-21096. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected.

### [CVE-2025-8715](#)

Improper neutralization of newlines in pg\_dump in PostgreSQL allows a user of the origin server to inject arbitrary code for restore-time execution as the client operating system account running psql to restore the dump, via psql meta-commands inside a purpose-crafted object name. The same attacks can achieve SQL injection as a superuser of the restore target server. pg\_dumpall, pg\_restore, and pg\_upgrade are also affected. Versions before PostgreSQL 17.6, 16.10, 15.14, 14.19, and 13.22 are affected. Versions before 11.20 are unaffected. CVE-2012-0868 had fixed this class of problem, but version 11.20 reintroduced it.

## Vulnerability Info

CVE No.	CVSS Score	Type of Vulnerability
<a href="#">CVE-2025-8713</a>	3.1	CWE-1230 Exposure of Sensitive Information Through Metadata
<a href="#">CVE-2025-8714</a>	8.8	CWE-829 Inclusion of Functionality from Untrusted Control Sphere
<a href="#">CVE-2025-8715</a>	8.8	CWE-93 Improper Neutralization of CRLF Sequences ('CRLF Injection')

Eviden is investigating the exact nature of these vulnerabilities to provide validated remediation.

## Affected products

Products	Fixed version	Status	Comments
PostgreSQL	13.22 14.19 15.14 16.10 17.6	Fixed	

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable if the above table is incomplete or erroneous. During its vulnerability analysis process, the information in this document is subject to change without notice to reflect new results of this analysis.

TBD (to be defined) indicates that a new version fixing the vulnerabilities is under study.

Unpatched means that the vulnerability is presumably present, but there is no plan to provide a fix. This can be investigated on demand.

## List of HPC Management products

Products	Fixed version	Status	Comment
SMC xScale	2.2	Fixed	Affected version: 1.6, 2.0, 2.1

## Recommendations

Eviden recommends applying its Technical States upgrade on its servers as soon as they are made available.

## Available Vendor Patches

No validated patch is available at the time. Eviden is working with its suppliers to distribute updates as soon as possible.

## Available Workarounds

Vendor indicated patches: 13.22, 14.19, 15.14, 16.10, 17.6

## Available Mitigations

No mitigation identified.

## Available Exploits/PoC

Eviden is not aware of any exploitation of the reported vulnerabilities.

## References

1. <https://www.postgresql.org/support/security/CVE-2025-8713/>
2. <https://www.postgresql.org/support/security/CVE-2025-8714/>
3. <https://www.postgresql.org/support/security/CVE-2025-8715/>
4. <https://www.cert.ssi.gouv.fr/avis/CERTFR-2025-AVI-0702/>
- 5.

## Glossary of terms

Term	Description
Mitigation	Refers to a setting, common configuration, or general best-practice, existing in a default state that could reduce the severity of exploitation of a vulnerability
Neutralization	The neutralization phase is the decision-making process during which the risk posed by an incident is evaluated.
PoC	Proof of Concept
Remediation	The remediation phase ends with the delivering of a qualified solution/update fixing the vulnerability without regression.
TI	Threat Intelligence
TLP	Traffic Light Protocol (TLP) FIRST Standards Definitions and Usage Guidance — Version 2.0. <a href="https://www.first.org/tlp/">https://www.first.org/tlp/</a>
Workaround	Refers to a setting or configuration change that does not correct the underlying vulnerability but would help block known attack vectors before you apply the update

## About this document

Eviden continuously monitors the security of its products. This Security Bulletin is shared under the constraints of the FIRST Traffic Light Protocol version 2.0 (TLP) to bring the attention of owners of the potentially affected Eviden products. Eviden recommends that all product owners determine whether the described situation is applicable to their individual case and take appropriate action.

Although Eviden tries to provide accurate and complete information, Eviden shall not be liable for technical or editorial errors contained in this Bulletin. The information is provided "as is" without warranty of any kind. To the extent permitted by the Law, neither Eviden nor its affiliates, subcontractors or suppliers will be liable for incidental damages, downtime cost, lost profits, damages relating to the procurement of substitute products or services, or damages for loss of data, or software restoration. Product and company names mentioned herein may be trademarks of their respective owners.

The information in this document is subject to change without notice. The version of this document will be incremented according to the changes:

- Neutralization security bulletins are numbered 0.x
- Privately disclosed Remediation security bulletins are numbered 1.x
- Publicly disclosed Remediation security bulletins are numbered 2.x

Updated versions of this document can be found on:

- <https://support.bull.com/ols/product/security/psirt>

## About Atos

Atos is a global leader in digital transformation with 105,000 employees and annual revenue of c. € 11 billion. European number one in cybersecurity, cloud and high-performance computing, the Group provides tailored end-to-end solutions for all industries in 69 countries. A pioneer in decarbonization services and products, Atos is committed to a secure and decarbonized digital for its clients. Atos is a SE (Societas Europaea) and listed on Euronext Paris.

The [purpose of Atos](#) is to help design the future of the information space. Its expertise and services support the development of knowledge, education and research in a multicultural approach and contribute to the development of scientific and technological excellence. Across the world, the Group enables its customers and employees, and members of societies at large to live, work and develop sustainably, in a safe and secure information space.

## About Eviden<sup>1</sup>

[Eviden](#) is a next-gen technology leader in data-driven, trusted and sustainable digital transformation with a strong portfolio of patented technologies. With worldwide leading positions in advanced computing, security, AI, cloud and digital platforms, it provides deep expertise for all industries in more than 47 countries. Bringing together 53,000 world-class talents, Eviden expands the possibilities of data and technology across the digital continuum, now and for generations to come. Eviden is an Atos Group company with an annual revenue of c. € 5 billion.

---

<sup>1</sup> Eviden business is operated through the following brands: AppCentrica, ATHEA, BullSequana, Cloudamize, Cloudreach, Cryptovision, DataSentics, Edifixio, Energy4U, Engage ESM, Evidian, Forensik, IDEAL GRP, IDnomic, In Fidem, Ipsotek, Maven Wave, Profit4SF, SEC Consult, Trustway, Visual BI, Worldgrid, X-Perion.  
Eviden is a registered trademark. © Eviden SAS, 2026.