BREAKING CYBERSECURITY NEWS: POSTGRESQL VULNERABILITY EXPLOITED ALONGSIDE BEYONDTRUST ZERO-DAY IN TARGETED ATTACKS

Vairav Cyber Security News Report

Date: 2025-02-14

Vairav Cyber Threat Intelligence Team

Vairav Technology Security Pvt. Ltd.

Thirbam Sadak 148

Baluwatar, Kathmandu

Phone: +977 4541540

Mobile: +977-9820105900

Email: mail@vairavtech.com

EXECUTIVE SUMMARY

A critical PostgreSQL vulnerability (CVE-2025-1094) enabling arbitrary code execution via SQL injection was exploited alongside a BeyondTrust zero-day (CVE-2024-12356). This flaw, affecting the psql tool, poses significant risks to organizations using PostgreSQL for database management, potentially leading to data breaches and operational disruptions.

DETAILS OF THE INCIDENT

Description: The vulnerability stems from how PostgreSQL handles invalid UTF-8 characters, thus opening the door to a scenario where an attacker could exploit an SQL injection by making use of a shortcut command "\!", which enables shell command execution.

Identification: Security researchers at Rapid7 identified the exploitation of CVE-2025-1094 during their investigation into CVE-2024-12356, a security flaw in BeyondTrust software.

Affected Entities/Industries: Organizations utilizing PostgreSQL as their database in versions prior to the patched releases.

Potential Impact: The exploitation of this vulnerability can lead to arbitrary code execution, allowing attackers to execute malicious commands on the affected systems. This poses significant risks, including data breaches, system compromise, and potential operational disruptions.

Exploitation Methods:

Attackers exploit the SQL injection flaw in PostgreSQL's psql tool to perform meta-commands, thereby controlling the operating system shell command that is executed. This method enables them to execute arbitrary code on the affected systems.

RECOMMENDED ACTIONS

Immediate Mitigation Steps

- Update PostgreSQL to the latest versions: 17.3, 16.7, 15.11, 14.16, or 13.19, which address CVE-2025-1094.
- Apply patches provided by BeyondTrust for their Privileged Remote Access and Remote Support products to mitigate CVE-2024-12356.

Security Best Practices

- Regularly update all software and systems to the latest versions to mitigate known vulnerabilities.
- Restrict access to database management tools and ensure only authorized personnel have access.
- Implement network segmentation to limit the potential impact of a compromised system.

For Advanced Security Teams

- Conduct thorough code reviews and vulnerability assessments to identify and remediate potential security flaws.
- Monitor system and network logs for unusual activities that may indicate exploitation attempts.
- Develop and test incident response plans to ensure rapid mitigation in case of a security breach.

ADDITIONAL RESOURCES AND OFFICIAL STATEMENTS

- https://www.rapid7.com/blog/post/2025/02/13/cve-2025-1094-postgresql-psql-sql-injection-fixed/
- https://nvd.nist.gov/vuln/detail/CVE-2025-1094

CONTACT US

Vairav Technology Security Pvt. Ltd.

Cyber Defender from the land of Gurkha

Thirbam Sadak 148, Baluwatar

Kathmandu, Nepal

Phone: +977-01-4541540

Mobile: +977-9820105900

Email: sales@vairavtech.com

Website: https://vairavtech.com