Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

PostgreSQL Flaw CVE-2025-1094 Joins BeyondTrust Zero-Day in Stealthy Attacks

Date of Publication	Admiralty Code	TA Number
February 17, 2025	A1	TA2025044

Summary

First Seen: January 27, 2025
Affected Products: PostgreSQL psql, BeyondTrust Privileged Remote Access (PRA) and BeyondTrust Remote Support (RS)
Actor: Silk Typhoon (aka Hafnium, Red Dev 13, ATK233, G0125, Operation Exchange Marauder)
Impact: A high-severity SQL injection vulnerability, CVE-2025-1094, has been discovered in PostgreSQL's interactive tool, psql. This flaw allows attackers to execute arbitrary SQL commands, which can escalate to arbitrary code execution (ACE) by exploiting psql's ability to run meta-commands. CVE-2025-1094 has played a crucial role in achieving remote code execution (RCE) in every tested scenario when chained with CVE-2024-12356, a recently patched vulnerability in BeyondTrust software. Additionally, CVE-2024-12356 and CVE-2024-12686 have been actively exploited by the Silk Typhoon threat group, which conducted reconnaissance and data theft operations.

CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2025-1094	PostgreSQL psql SQL Injection Vulnerability	PostgreSQL psql	✓	✗	✓
CVE-2024-12356	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and BeyondTrust Remote Support (RS)	✓	✓	✓
CVE-2024-12686	BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS) OS Command Injection Vulnerability	BeyondTrust Privileged Remote Access (PRA) and BeyondTrust Remote Support (RS)	✓	✓	✓

Vulnerability Details

#1 A critical SQL injection vulnerability, CVE-2025-1094, has been identified in PostgreSQL's interactive tool, psql. The issue stems from flaws in PostgreSQL's input escaping mechanisms, which, under certain conditions, fail to properly sanitize untrusted input, leaving systems vulnerable to SQL injection.

#2 This flaw occurs when invalid UTF-8 characters are processed, particularly when PostgreSQL's string escaping functions are used with mismatched encodings. This loophole enables attackers to inject SQL commands and escalate their attack to arbitrary code execution (ACE) by exploiting psql's meta-commands, which allow system-level shell commands to be executed.

#3 The vulnerability came to light during an investigation into CVE-2024-12356, a Command Injection flaw affecting BeyondTrust Privileged Remote Access (PRA) and Remote Support (RS). Researchers found that CVE-2024-12356 exploits relied on CVE-2025-1094 to achieve ACE, making it a critical component of the attack chain. Additionally, it's confirmed that CVE-2025-1094 can be exploited on its own to achieve remote code execution in vulnerable BeyondTrust RS environments, without needing to chain it with CVE-2024-12356.

#4 Moreover, CVE-2024-12686, a command injection vulnerability in BeyondTrust PRA and RS, can be exploited by attackers with administrative privileges to upload and execute malicious files. Both CVE-2024-12356 and CVE-2024-12686 have been actively exploited by the Silk Typhoon threat group, which conducted reconnaissance and data theft operations against the U.S. Treasury Department.

#5 Given the critical nature of CVE-2025-1094 and its exploitation in targeted attacks, organizations using PostgreSQL, BeyondTrust PRA, or RS should apply security updates immediately and review their system configurations to minimize risk.

Vulnerabilities

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2025-1094	PostgreSQL Versions Before 17.3, 16.7, 15.11, 14.16, and 13.19	cpe:2.3:a:postgresql:postgresql:*:*:*:*:*:*:*:*	CWE-149
CVE-2024-12356	BeyondTrust Privileged Remote Access (PRA) Versions 24.3.1 and earlier, BeyondTrust Remote Support (RS) Versions 24.3.1 and earlier	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:*	CWE-77
CVE-2024-12686	BeyondTrust Privileged Remote Access (PRA) Version 24.3.1 and earlier, BeyondTrust Remote Support (RS) Version 24.3.1 and earlier	cpe:2.3:a:beyondtrust:privileged_remote_access:*:*:*:*:*:*:*:* cpe:2.3:a:beyondtrust:remote_support:*:*:*:*:*:*:*:*	CWE-78

Recommendations

Stay Updated: Update PostgreSQL to a fixed version to prevent potential exploits against CVE-2025-1094. If you're using BeyondTrust Privileged Remote Access (PRA) or Remote Support (RS), make sure to apply the latest updates immediately to protect against CVE-2024-12356 and CVE-2024-12686.

Limit Access: Limit the use of the PostgreSQL interactive tool (psql) to trusted users only. Restrict or disable meta-commands within psql to avoid the risk of executing arbitrary commands.

Harden Database Security: Strengthen database security by enforcing least privilege access controls to restrict SQL execution. Deploy Web Application Firewalls (WAFs) or Intrusion Detection Systems (IDS) to identify and block SQL injection attempts.

Potential MITRE ATT&CK TTPs

TA0043 Reconnaissance	**TA0042** Resource Development	**TA0001** Initial Access	**TA0002** Execution
T1588 Obtain Capabilities	**T1588.006** Vulnerabilities	**T1588.005** Exploits	**T1059** Command and Scripting Interpreter
T1190 Exploit Public-Facing Application	**T1133** External Remote Services		

Indicators of Compromise (IOCs)

TYPE	VALUE
IPv4	24[.]144[.]114[.]85, 142[.]93[.]119[.]175, 157[.]230[.]183[.]1, 192[.]81[.]209[.]168

Patch Details

- To address CVE-2025-1094, PostgreSQL users should upgrade to PostgreSQL Versions 17.3, 16.7, 15.11, 14.16, or 13.19.

- For CVE-2024-12356, apply the appropriate patch based on the product version:
  Privileged Remote Access (PRA): Install PRA patch BT24-10-ONPREM1 or BT24-10-ONPREM2, depending on the PRA version.
  Remote Support (RS): Install RS patch BT24-10-ONPREM1 or BT24-10-ONPREM2, based on the RS version.
- For CVE-2024-12686, apply the appropriate patch based on the product version:
  Privileged Remote Access (PRA): Install PRA patch BT24-11-ONPREM1, BT24-11-ONPREM2, BT24-11-ONPREM3, BT24-11-ONPREM4, BT24-11-ONPREM5, BT24-11-ONPREM6, BT24-11-ONPREM7, dependent on PRA version.
  Remote Support (RS): Install RS patch BT24-11-ONPREM1, BT24-11-ONPREM2, BT24-11-ONPREM3, BT24-11-ONPREM4, BT24-11-ONPREM5, BT24-11-ONPREM6, BT24-11-ONPREM7, dependent on RS version.

Links: https://www.postgresql.org/support/security/CVE-2025-1094/

https://www.beyondtrust.com/trust-center/security-advisories/bt24-10

https://www.beyondtrust.com/trust-center/security-advisories/bt24-11

References

https://www.rapid7.com/blog/post/2025/02/13/cve-2025-1094-postgresql-psql-sql-injection-fixed/

https://www.postgresql.org/support/security/CVE-2025-1094/

https://www.beyondtrust.com/trust-center/security-advisories/bt24-10

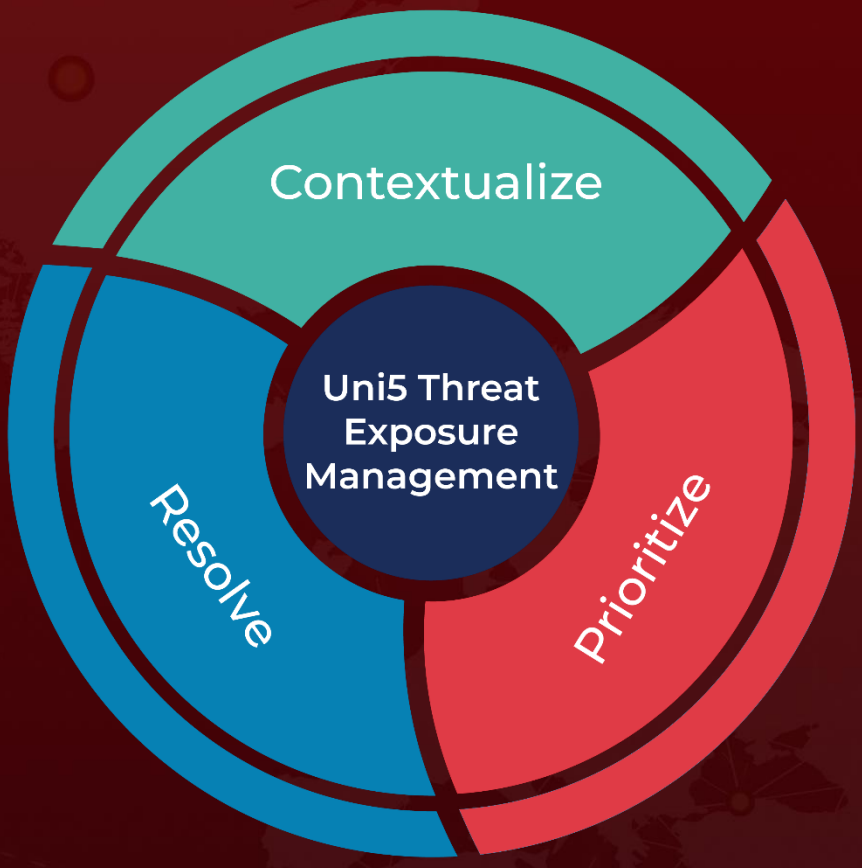
https://www.beyondtrust.com/trust-center/security-advisories/bt24-11

BeyondTrust Remote Support SaaS Service Security… | BeyondTrust

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

February 17, 2025 • 7:20 AM

More at www.hivepro.com