Security changelog

Fixed in ClickHouse v26.10.3.7, 2026-10-30

CVE-2026-116366

An issue has been discovered in ClickHouse Server that, under certain conditions, could allow an unauthenticated user with network access to execute arbitrary code on the ClickHouse Server.

Fix has been pushed to the following open-source versions: v26.3.62.3-lts, v26.8.36.3-lts, v26.9.27.3-stable, v26.10.3.7-stable.

A fix for this vulnerability has been applied to all ClickHouse Cloud and BYOC deployments.

Credits: Elshad Toklayev.

Fixed in ClickHouse v25.1.5.5, 2025-01-05

CVE-2025-1385

When the library bridge feature is enabled, the clickhouse-library-bridge exposes an HTTP API on localhost. This allows clickhouse-server to dynamically load a library from a specified path and execute it in an isolated process. Combined with the ClickHouse table engine functionality that permits file uploads to specific directories, a misconfigured server can be exploited by an attacker with privileges to access both table engines, allowing them to execute arbitrary code on the ClickHouse server.

Credits: Arseniy Dugin

Fixed in ClickHouse v24.5, 2024-08-01

CVE-2024-6873

It is possible to redirect the execution flow of the ClickHouse server process from an unauthenticated vector by sending a specially crafted request to the ClickHouse server native interface. This redirection is limited to what is available within a 256-byte range of memory at the time of execution. This vulnerability was identified through our Bugbounty program and no known Proof of Concept Remote Code Execution (RCE) code has been produced or exploited.

Fix has been pushed to the following open-source versions: v23.8.15.35-lts, v24.3.4.147-lts, v24.4.2.141-stable, v24.5.1.1763, v24.6.1.4423-stable

ClickHouse Cloud uses different versioning and a fix for this vulnerability was applied to all instances running v24.2 onward.

Credits: malacupa (Independent researcher)

Fixed in ClickHouse v24.1, 2024-01-30

CVE-2024-22412

When toggling between user roles while using ClickHouse with query cache enabled, there is a risk of obtaining inaccurate data. ClickHouse advises users with vulnerable versions of ClickHouse not to use the query cache when their application dynamically switches between various roles.

v24.6.2.54353.

Credits: Evan Johnson and Alan Braithwaite from Runreveal team - More information can be found on their blog post.

Fixed in ClickHouse v23.10.5.20, 2023-11-26

CVE-2023-47118

A heap buffer overflow vulnerability affecting the native interface running by default on port 9000/tcp. An attacker, by triggering a bug in the T64 compression codec, can cause the ClickHouse server process to crash. This vulnerability can be exploited without the need to authenticate.

Fix has been pushed to the following open-source versions: v23.10.2.13, v23.9.4.11, v23.8.6.16, v23.3.16.7

ClickHouse Cloud uses different versioning and a fix for this vulnerability was applied at v23.9.2.47475.

Credits: malacupa (Independent researcher)

CVE-2023-48298

An integer underflow vulnerability in the FPC compressions codec. An attacker can use it to cause the ClickHouse server process to crash. This vulnerability can be exploited without the need to authenticate.

Fix has been pushed to the following open-source versions: v23.10.4.25, v23.9.5.29, v23.8.7.24, v23.3.17.13.

ClickHouse Cloud uses different versioning and a fix for this vulnerability was applied at v23.9.2.47475.

A heap buffer overflow vulnerability affecting the native interface running by default on port 9000/tcp. An attacker, by triggering a bug in the Gorilla codec, can cause the ClickHouse server process to crash. This vulnerability can be exploited without the need to authenticate.

Fix has been pushed to the following open-source versions: v23.10.5.20, v23.9.6.20, v23.8.8.20, v23.3.18.15.

ClickHouse Cloud uses different versioning and a fix for this vulnerability was applied at v23.9.2.47551.

Credits: malacupa (Independent researcher)

Fixed in ClickHouse 22.9.1.2603, 2022-09-22

CVE-2022-44011

A heap buffer overflow issue was discovered in ClickHouse server. A malicious user with ability to load data into ClickHouse server could crash the ClickHouse server by inserting a malformed CapnProto object.

Fix has been pushed to version 22.9.1.2603, 22.8.2.11, 22.7.4.16, 22.6.6.16, 22.3.12.19

Credits: Kiojj (independent researcher)

CVE-2022-44010

A heap buffer overflow issue was discovered in ClickHouse server. An attacker could send a specially crafted HTTP request to the HTTP Endpoint (listening on port 8123 by default), causing a heap-based buffer overflow that crashes the ClickHouse server process. This attack does not require authentication.

Fix has been pushed to version 22.9.1.2603, 22.8.2.11, 22.7.4.16, 22.6.6.16, 22.3.12.19

CVE-2021-43304

Heap buffer overflow in ClickHouse's LZ4 compression codec when parsing a malicious query. There is no verification that the copy operations in the LZ4::decompressImpl loop and especially the arbitrary copy operation `wildCopy<copy_amount>(op, ip, copy_end)`, don't exceed the destination buffer's limits.

Credits: JFrog Security Research Team

CVE-2021-43305

Heap buffer overflow in ClickHouse's LZ4 compression codec when parsing a malicious query. There is no verification that the copy operations in the LZ4::decompressImpl loop and especially the arbitrary copy operation `wildCopy<copy_amount>(op, ip, copy_end)`, don't exceed the destination buffer's limits. This issue is very similar to CVE-2021-43304, but the vulnerable copy operation is in a different wildCopy call.

Credits: JFrog Security Research Team

CVE-2021-42387

Heap out-of-bounds read in ClickHouse's LZ4 compression codec when parsing a malicious query. As part of the LZ4::decompressImpl() loop, a 16-bit unsigned user-supplied value ('offset') is read from the compressed data. The offset is later used in the length of a copy operation, without checking the upper bounds of the source of the copy operation.

Credits: JFrog Security Research Team

CVE-2021-42388

Heap out-of-bounds read in ClickHouse's LZ4 compression codec when parsing a malicious query. As part of the LZ4::decompressImpl() loop, a 16-bit unsigned user-supplied value

CVE-2021-42389

Divide-by-zero in ClickHouse's Delta compression codec when parsing a malicious query. The first byte of the compressed buffer is used in a modulo operation without being checked for 0.

Credits: JFrog Security Research Team

CVE-2021-42390

Divide-by-zero in ClickHouse's DeltaDouble compression codec when parsing a malicious query. The first byte of the compressed buffer is used in a modulo operation without being checked for 0.

Credits: JFrog Security Research Team

CVE-2021-42391

Divide-by-zero in ClickHouse's Gorilla compression codec when parsing a malicious query. The first byte of the compressed buffer is used in a modulo operation without being checked for 0.

Credits: JFrog Security Research Team

Fixed in ClickHouse 21.4.3.21, 2021-04-12

CVE-2021-25263

An attacker that has CREATE DICTIONARY privilege, can read arbitary file outside permitted directory.

Fixed in ClickHouse Release 19.14.3.3, 2019-09-10

CVE-2019-15024

An attacker that has write access to ZooKeeper and who can run a custom server available from the network where ClickHouse runs, can create a custom-built malicious server that will act as a ClickHouse replica and register it in ZooKeeper. When another replica will fetch data part from the malicious replica, it can force clickhouse-server to write to arbitrary path on filesystem.

Credits: Eldar Zaitov of Yandex Information Security Team

CVE-2019-16535

An OOB read, OOB write and integer underflow in decompression algorithms can be used to achieve RCE or DoS via native protocol.

Credits: Eldar Zaitov of Yandex Information Security Team

CVE-2019-16536

Stack overflow leading to DoS can be triggered by a malicious authenticated client.

Credits: Eldar Zaitov of Yandex Information Security Team

Fixed in ClickHouse Release 19.13.6.1, 2019-09-20

CVE-2019-18657

Table function `url` had the vulnerability allowed the attacker to inject arbitrary HTTP headers in the request.

CVE-2018-14672

Functions for loading CatBoost models allowed path traversal and reading arbitrary files through error messages.

Credits: Andrey Krasichkov of Yandex Information Security Team

Fixed in ClickHouse Release 18.10.3, 2018-08-13

CVE-2018-14671

unixODBC allowed loading arbitrary shared objects from the file system which led to a Remote Code Execution vulnerability.

Credits: Andrey Krasichkov and Evgeny Sidorov of Yandex Information Security Team

Fixed in ClickHouse Release 1.1.54388, 2018-06-28

CVE-2018-14668

“remote” table function allowed arbitrary symbols in “user”, “password” and “default_database” fields which led to Cross Protocol Request Forgery Attacks.

Credits: Andrey Krasichkov of Yandex Information Security Team

Fixed in ClickHouse Release 1.1.54390, 2018-07-06

CVE-2018-14669

ClickHouse MySQL client had “LOAD DATA LOCAL INFILE” functionality enabled that allowed a malicious MySQL database read arbitrary files from the connected ClickHouse server.

CVE-2018-14670

Incorrect configuration in deb package could lead to the unauthorized use of the database.

Credits: the UK's National Cyber Security Centre (NCSC)

Was this page helpful? Yes No Suggest edits Raise issue

Previous
2017
Changelog for 2017