Everything You Need to Know About the Cloudflare Outage

November 20, 2025

On November 18, 2025, a widespread service disruption impacted Cloudflare's global network, rendering a significant portion of the internet inaccessible for approximately six hours. While initial traffic patterns mimicked those of a hyper-scale distributed denial of service (DDoS) attack, forensic analysis reportedly indicated that the root cause was an internal logic failure in their bot management system.[1]

This advisory breaks down the technical mechanics of the outage, the specific database anomalies that triggered the failure, and the implications for organizations relying on single-vendor security architectures. This advisory reflects information available as of November 19, 2025.

Key Insights

- **Security as the Single Point of Failure:** The outage occurred within the protection layer itself. The system experienced a "fail-closed" event, meaning that when the bot management logic crashed, it defaulted to blocking all traffic rather than bypassing the check, severing connectivity for legitimate users.
- **Cyclical Instability:** The confusing "flapping" behavior, in which services recovered and then crashed again, was the result of a timing conflict between two processes. The bot management configuration file was regenerated every five minutes, while the database permission update was rolled out gradually across nodes. This meant service stability varied depending on which database node processed the request at any given moment.
- **The Case for Diversification:** Relying heavily on a single vendor for critical path services (DNS, WAF, Zero Trust) concentrates risk. This incident highlights the importance of architectural redundancy and "break-glass" mechanisms that allow traffic to bypass a failed security layer during vendor-specific outages.

Background

The incident began at 11:20 UTC on November 18, 2025. Users globally reported HTTP 5xx errors when attempting to access properties protected by Cloudflare. The disruption effectively blocked legitimate traffic while rendering security dashboards and authentication services, such as Cloudflare Access and Turnstile, unavailable.[2]

Unlike typical outages caused by physical infrastructure failures, this event was characterized by a "flapping" pattern in which services would recover briefly before failing again. This behavior complicated immediate diagnosis and response efforts.[3]

The Root Cause: A ClickHouse Permission Anomaly

The following analysis is based solely on publicly available information and is not intended to make any independent factual assertions regarding Cloudflare or its products.

The outage was triggered by a routine maintenance update to the permissions within Cloudflare's **ClickHouse** database cluster, which powers analytics and bot detection.[4]

The reported failure occurred in the system that compiles the security rules used to screen website traffic. Under normal circumstances, this system reads these rules from a single, consolidated catalog. However, a routine update incorrectly granted the system access to the raw storage layer that sits beneath that catalog. Because the system began reading from both sources simultaneously, the primary catalog and the raw storage, it inadvertently listed every rule twice, creating a file full of duplicate instructions that the network could not process

According to public reports, this duplication instantly doubled the size of the configuration file. Cloudflare's edge proxy software, built in Rust, enforced a hard-coded limit of 200 features for this file. When the oversized file exceeded this cap, it triggered a critical error (a **Rust panic**), causing the core traffic-handling processes to crash immediately.[1]

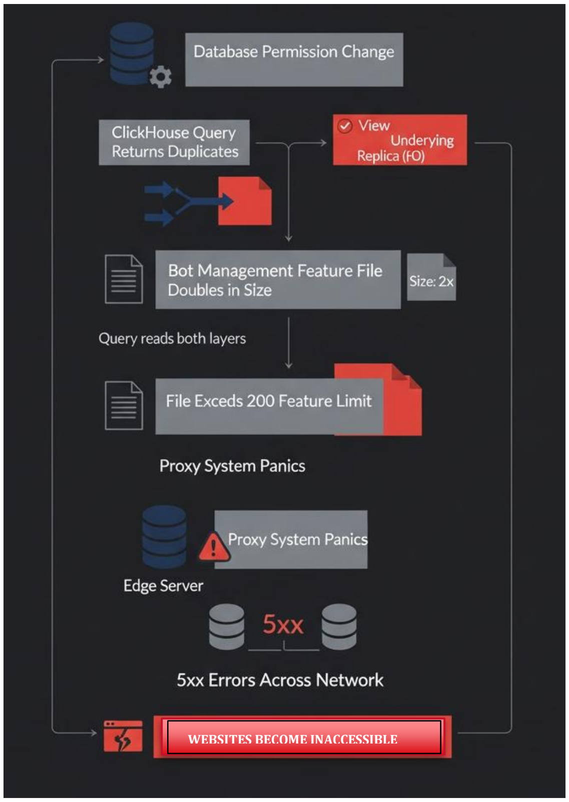
Database Permission Change
ClickHouse Query Returns Duplicates
View Underying Replica (FO)
Bot Management Feature File Doubles in Size
Size: 2x
Query reads both layers
File Exceds 200 Feature Limit
Proxy System Panics
Proxy System Panics
Edge Server
5xx
5xx Errors Across Network
WEBSITES BECOME INACCESSIBLE

Figure 1: Cloudflare outage chain of events (Source: Radware)

The Intermittent Loop ("Flapping")

A defining characteristic of this incident was its intermittent nature. The network did not simply go dark; it cycled between failure and recovery. The interaction between the update rollout and the generation cycle drove this behavior:

- **The Cycle:** The bot management feature file is regenerated every five minutes.[2]
- **The Rollout:** The database permission change was applied gradually across the cluster. Some nodes had new (buggy) permissions, while others retained the old configuration.
- **The Result:** If the generation job queried a node *without* the update, a valid file was produced, and traffic flowed. If it queried a node *with* the update, a corrupt file was produced, causing the edge to crash. This created a global situation in which internet connectivity depended on which database node handled the query during that five-minute window.[2]

Impact on Cyberthreat Mitigation

According to available reports, this incident represents a "fail-closed" scenario. While the failure technically prevented malicious traffic from passing, it did so by sacrificing availability entirely, which violates the Availability pillar of the CIA triad.[3]

Critically, the outage originated within the security layer itself. The incident reports services designed to mitigate threats became the point of failure:

- **Bot Management:** This became non-functional and the source of the crash.
- **Turnstile:** The CAPTCHA replacement service failed, locking out users requiring validation.
- **Zero Trust Access:** Authentication workflows broke, preventing administrators from accessing internal tools to manage the crisis.[1]

Recommendations

In light of this event, Radware recommends organizations review their resilience strategies to minimize reliance on single points of failure:

- **Diversify Security Architecture:** Relying on a single vendor for DNS, WAF and bot management concentrates risk. Consider a multi-vendor or hybrid approach to ensure redundancy.
- **Implement Failover Logic:** Organizations should maintain "break-glass" procedures or secondary CDN configurations that can bypass a failed security layer to restore core business continuity during a vendor-specific outage.
- **External Monitoring:** Utilize third-party monitoring tools that operate outside your primary CDN's infrastructure to detect and diagnose connectivity issues independently of vendor status pages.

Resources List

[1] Matthew Prince, "Cloudflare outage on November 18, 2025 (Post Mortem)," *Cloudflare Blog*, November 18, 2025. https://blog.cloudflare.com/18-november-2025-outage/

[2] Roundz.ai Research Team, "Postmortem: A Deep Dive into Cloudflare's November 2025 Outage," *Roundz.ai*, November 19, 2025. https://roundz.ai/blog/postmortem-deep-dive-cloudflare-november-2025-outage

[3] The Cyber Express, "Inside the Cloudflare Outage of November 18, 2025," *The Cyber Express*, November 19, 2025. https://thecyberexpress.com/cloudflare-outage-november-18-2025-analysis/

[4] GBHackers, "Cloudflare Reveals Full Technical Explanation of Major Internet Outage," *GBHackers On Security*, November 1, 2025. https://gbhackers.com/cloudflare-full-technical-explanation-of-internet-outage/

EFFECTIVE WEB APPLICATION SECURITY ESSENTIALS

Full OWASP Top 10 coverage against defacements, injections, etc.

Low false-positive rate using negative and positive security models for maximum accuracy

Auto-policy generation capabilities for the broadest coverage with the lowest operational effort

Bot protection and device fingerprinting capabilities to overcome dynamic IP attacks and achieve improved bot detection and blocking

Securing APIs by filtering paths, understanding XML and JSON schemas for enforcement, and using activity tracking mechanisms to trace bots and guard internal resources

Flexible deployment options, including on-premises, out-of-path, virtual or cloud-based deployments

LEARN MORE AT RADWARE'S SECURITY RESEARCH CENTER.

To know more about today's attack vector landscape, understand the business impact of cyberattacks, or learn more about emerging attack types and tools, visit Radware's **Security Research Center**. Additionally, visit Radware's **Quarterly DDoS & Application Threat Analysis Center** for quarter-over-quarter analysis of DDoS and application attack activity based on data from Radware's cloud security services and threat intelligence.

THIS REPORT CONTAINS ONLY PUBLICLY AVAILABLE INFORMATION, WHICH IS PROVIDED FOR GENERAL INFORMATION PURPOSES ONLY. ALL INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATION OR WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, ANY IMPLIED WARRANTIES THAT THIS REPORT IS ERROR-FREE OR ANY IMPLIED WARRANTIES REGARDING THE ACCURACY, VALIDITY, ADEQUACY, RELIABILITY, AVAILABILITY, COMPLETENESS, FITNESS FOR ANY PARTICULAR PURPOSE, OR NON-INFRINGEMENT. USE OF THIS REPORT, IN WHOLE OR IN PART, IS AT THE USER'S SOLE RISK. RADWARE AND/OR ANYONE ON ITS BEHALF SPECIFICALLY DISCLAIMS ANY LIABILITY IN RELATION TO THIS REPORT, INCLUDING WITHOUT LIMITATION, FOR ANY DIRECT, SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR EXEMPLARY DAMAGES, LOSSES AND EXPENSES ARISING FROM OR IN ANY WAY RELATED TO THIS REPORT, HOWEVER CAUSED, AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHER THEORY OF LIABILITY, EVEN IF IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, LOSSES OR EXPENSES. **CHARTS USED OR REPRODUCED SHOULD BE CREDITED TO RADWARE.**