AKASH KUMAR BANIK 24MCA0242

PMCA614L - SOFTWARE TESTING TH DA-1

RECENT SOFTWARE FAILURES [2020 - 2025]

Introduction:

Software Failures in critical and expensive projects can have far reaching consequences, from financial losses to safety risks. This report compiles case studies to illustrate how inadequate testing practices contributed to these failures and offers insights into improving software reliability.

CASE STUDY 1 : Zoom Security Issues (2020) →

Description: In 2020, Zoom Video Communications faced significant security scrutiny as its usage surged due to the COVID-19 pandemic, reaching 300 million daily users by April 2020 from 10 million in December 2019. This rapid growth exposed several security & privacy issues, including "Zoombombing", where unauthorized users disrupted meetings with inappropriate content, and the misrepresentation of end-to-end encryption, which was not truly end-to-end, allowing potential access to meeting content.

Cause: The primary cause was the platform's focus on user-friendliness and rapid scaling, which outpaced security measures. Features like open meeting links facilitated ease of use but made the platform vulnerable to abuse. Security researchers identified vulnerabilities, and the New York State Attorney General's investigation revealed inadequate privacy practices.

Impact : The impact was significant, with disruptions to meetings, privacy breaches, and loss of trust among users. Large organisations, including government & co-orporations like Google, banned or restricted Zoom use in April 2020, citing security flaws. This led to a class-action lawsuit from investors for fake security claims, affecting Zoom's reputation & stock market volatility.

Conclusion : This case highlights the need for comprehensive security testing, including penetration testing to identify vulnerabilities like Zoombombing and privacy impact assessments to ensure transparent encryption claims. Regular code reviews and penetration testing, as mandated by the NYAG agreement, could have mitigated these issues.

CASE STUDY 2 : Log4j Vulnerability (2021) →

Description : In December 2021, a critical remote code execution (RCE) vulnerability, known as Log4Shell (CVE-2021-44228), was discovered in the Apache Log4j library, widely used in Java-based systems for logging. This vulnerability allowed attackers to execute arbitrary code by injecting malicious content into log messages, affecting versions 2.0-beta9 to 2.14.1.

Cause : The flaw was in the JNDI lookup feature, which did not properly sanitize inputs, enabling attackers to exploit it for RCE. This was identified as a zero-day vulnerability, meaning it was exploited before a patch was available, highlighting inadequate security testing during development.

Impact: The impact was massive, with millions of systems vulnerable, leading to widespread exploitation by cybercriminals. The Federal Trade Commission warned companies of legal risks, and research in 2023 showed nearly 2 in 5 applications still running vulnerable versions, indicating long-term effects on cybersecurity.

Conclusion: This incident underscores the importance of security testing for third-party libraries, including static code analysis to detect input validation issues and dynamic testing to simulate attack scenarios. Timely patching and vulnerability management, supported by automated testing, could have reduced the exposure.

Case Study 3: FAA NOTAM Database Outage (2023)

Description: On January 11, 2023, the Federal Aviation Administration (FAA) experienced a major outage in its Notice to Air Mission (NOTAM) system, critical for providing safety alerts to pilots. A contractor unintentionally deleted files while attempting to synchronize the primary and backup databases, leading to a nationwide ground stop, the first in over 20 years.

Cause: The cause was a human error during database maintenance, specifically during the synchronization process, where files were deleted, disrupting the system's operation. The FAA found no evidence of a cyberattack, confirming it as an operational mistake.

FAA NOTAM Outage Details →

Aspect	Details
Date	– January 11, 2023
System Affected	– Notice to Air Missions (NOTAM)
Cause	– Contractor deleted files during synch
Impact	– Nationwide ground stop, halting all flight takeoffs.
Response	– FAA enhanced system resilience, no cyberattack evidence.

Impact: The outage halted all US flight takeoffs, causing significant operational disruptions and financial losses for airlines and passengers, with ripple effects on the aviation industry.

Conclusion: This case emphasizes the need for testing backup and recovery procedures, including database integrity checks and validation of synchronization processes. Automated testing could ensure that such errors are caught before deployment, and operational testing could verify human procedures.

CASE STUDY 4 : NYSE Backup Server Failure (2023)

Description: On January 24, 2023, the New York Stock Exchange (NYSE) experienced a significant disruption when an employee failed to properly shut down a backup server at its Chicago data center, over 700 miles from Wall Street. This error caused wild market swings, affecting over 250 companies, with stock prices swinging by 25 percentage points in minutes.

Cause: The failure was due to a procedural mistake in disaster recovery management, where the backup systems was not turned off, leading to unintended interference with the live trading systems. This was a human error, not a technical flaw in the software itself.

NYSE Backup Server Failure Details →

- Date – January 24, 2023.
- Location – Cermak Road, Chicago
- Cause – Employee failed to shut down backup server.
- Impact – Market swings, cancelled trades, financial losses.
- Response – Cancelled trades, $500,000/month compensation fund.

Impact: The incident led to the cancellation of thousands of trades, with claims for compensation due by Friday, three days after the event, and decisions by the end of the month. It caused significant financial losses for affected companies and traders, highlighting the fragility of financial systems.

Conclusion: This case points to the need for operational testing and disaster recovery testing to ensure procedures are correctly followed. Automation could reduce human error, and regular drills could verify backup system management, ensuring stability in critical financial operations.

Case Study 5 : CrowdStrike Global IT Outage (2024)

Description : On July 19, 2024, American cybersecurity company CrowdStrike distributed a faulty update to its Falcon Sensor security software, which is widely used to protect systems against potential threats. This update caused widespread problems with Microsoft Windows computers running the software, leading to approximately 8.5 million systems crashing and being unable to properly restart. This event has been described as the largest outage in the history of IT and "historic in scale". The outage disrupted daily life, businesses, and governments around the world, affecting industries such as airlines, airports, banks, hotels, hospitals, manufacturing, stock markets, broadcasting, gas stations, retail stores, and more, as well as government services like Emergency services and websites.

Cause : The root cause was a modification to Channel File 291, which led to an out-of-bounds memory read and an invalid page fault in the Windows sensor client, causing systems to enter a bootloop or recovery mode. This issue arose because the update passed validation due to a bug in CrowdStrike's content verification ~~software~~, which had been tested and released in March 2024. CrowdStrike's preliminary incident review, published on August 06, 2024, detailed that the conditions included a mismatch between the number of input fields in the IPC Template Type and the actual inputs provided by the sensor code, with a runtime array bounds check missing in the Content Interpreter and a logic error in the Content Validator. CrowdStrike CEO George Kurtz confirmed on the same day that it was not a cyberattack, emphasizing

it was a software error.

Impact: The impact was massive, with approximately 8.5 million Microsoft Windows devices affected, representing less than 1% of all Windows devices globally, as reported by Microsoft on July 20, 2024. The outage led to significant disruptions:

- Aviation → Over 5078 flights were cancelled on July 19, accounting for 4.6% of scheduled flights, with airlines like Delta, United, and American grounding operations temporarily. Delta reported cancelling over 7000 flights over 5 days, affecting 1.3 million passengers, with costs estimated at $500 million ($380 million lost revenue, $170 million expense).
- Financial Sector → Banks faced disruptions, with reports of payment failures and incorrect balances displayed, impacting customer transactions.

Many other sectors were also impacted massively including the Healthcare Services, Emergency Services, as well as Broadcasting Sector.

The worldwide financial damage has been estimated atleast US $10 billion, with UK costs ranging from $2.18 - 2.96 billion and top 500 US companies (excluding Microsoft) facing approximately $5.4 billion in losses, with insured losses estimated at $540 million - 1.08 billion.

CrowdStrike identified the issue and reverted the update at 5:27 UTC, with a fix deployed by 9:45 UTC. The remediation process involved rebooting affected systems while connected to a network (ideally Ethernet), with multiple reboots

required in some cases. If systems remained in a bootloop, users were instructed to boot into safe boot mode on Windows Recovery Environment and delete .sys files beginning with C-00000291 - at %windir%\System32\drivers\CrowdStrike\ with a timestamp of 04:09 UTC. Microsoft recommended restoring backups from before July 18, 2024 to recover systems. However because of many affected computers required manual intervention, outages continued to linger for days, with businesses expecting several days to restore all systems fully.

Conclusion: The incident raised significant questions about the IT sector's reliance on centralized systems and the risks of software monocultures, particularly Microsoft Windows, which reduced resiliency. Experts suggested the need for redundancy, decentralized or federated systems, and regulatory measures to promote diversity and competition. Cybersecurity expert Andrew Plato argued that monocultures are not positive for security due to standardized updates, while others like Ciaran Martin and Gregory Falco emphasized the fragility and advocated for diverse systems. Speculations arose that the update was not tested in a sandbox, potentially leading to demands for changes in update push models without IT intervention. The incident also highlighted the need for Thorough Testing of Updates, Robust Validation Processes, Redundancy and Diversity in software solutions and also Contingency Planning.

REFERENCES →

Case Study - 1 :

(i) Tom's Guide Zoom Security & Privacy, detailing privacy & security flaws
tomsguide.com / news / zoom - security - privacy - woes.

(ii) Sigmund Software Zoom Security Issues, discussing vulnerabilities during the pandemic.
sigmundsoftware.com / blog / zoom - security - issues - coronavirus /

(iii) BBC News Zoom Company apology, covering Zoom's response to security criticisms.
bbc.com / news / technology - 52133349.

Case Study - 2 :

(iv) NCSC Log4j guidance, offering official cybersecurity advice.
ncsc.gov.uk / information / log4j - vulnerability - what - everyone - needs - to - know /

(v) FTC Log4j warning, warning companies of legal risks.
ftc.gov / policy / advocacy - research / tech - at - ftc / 2022 / 01 / ftc - warns - companies - remediate - log4j - security - vulnerability

(vi) Builtin Log4j explanation, explaining the technical details.
builtin.com / articles / log4j - vulnerability - explained.

Case Study - 3 :

(vii) CNN FAA Outage cause, detailing the incident.
cnn.com / 2023 / 01 / 19 / business / faa - notam - outage / index.html.

(viii) Computerworld FAA Outage, covering recovery efforts.
computerworld.com / article / 3685211 / us - flights - resume - after - system - failure - causes - faa - to - halt - air - travel.html

Case Study - 4 :

(IX) Bloomberg NYSE failure details, providing detailed analysis.
bloomberg.com / news / articles / 2023-01-25 / nyse-mayhem-traced-to-a-staffer-who-left-a-backup-system-running.

Case Study - 5 :

(X) Wikipedia CrowdStrike Outages, offering an overview.
wikipedia.org / wiki / 2024_CrowdStrike-related_IT_outages.

(XI) CrowdStrike Root Cause Analysis, detailing the technical cause.
crowdstrike.com / wp-content / uploads / 2024 / 08 / Channel-File-291-incident-Root-Cause-Analysis-08.06.2024.pdf.

(XII) The Register CrowdStrike lessons, analyzing lessons learned.
theregister.com / 2024 / 07 / 03 / crowdstrike_lessons_to_learn /.

(XIII) CrowdStrike Remediation Hub, providing recovery guidance.
crowdstrike.com / falcon-content-update-remediation-and-guidance-hub /

(XIV) BBC News Russia and China impact, discussing global effects.
bbc.com / news / articles / c3g01y047pdo.