10 Biggest Software Bugs and Tech Fails of 2021

Problem	Cause of the problem	solution
T-Mobile data breach: A 21-year old Hacker hacked their server and got all the current and former customer's data including name,dob,govt id,address	Its is due to unprotected router.thus the hacker was able to use that router and get into thier server and steal all the informations of the customers	Thus it should have an good protocol to protect the breach,we should do Security testing
Slack's New Feature: Slack introduced a new feature which help users to message or send anything who's outside of thier organization even though It's a good feature but there was an backlash	It is due to now the pepole can communicate with anyone outside their organization thus it can lead to data breach and sharing of some important data is possible thus their raised an backlash	Better solution can be for this is like we sholud have This feature for some higher level hierarchy person in an organization if he needs to contact some clients like he can have that feature and other should have not this feature
TikTok Gltich: On May 3 TikTok had an some technical issue.Due to this TikTok account holders follower account was reset to zero and was not able to access the app properly.And they wanted tiktok to recover thier account and followers and solve this by trending the hashtag #TikTokDown	There can be many possible reason for this glitch.it can be due to some software updates,or due to overload in the server or database connection failure or due to some third parties api they were using to collect some data may malfunction	Solution can be for this Implement enhanced software testing and a robust incident response plan to catch bugs early and communicate effectively with users during outages.
The Colonial Pipeline cyber attack in 2021 disrupted fuel supply across the East Coast, leading to gasoline shortages and price spikes after hackers gained access to the network and demanded a ransom.	The attack was facilitated by a lack of multifactor authentication (MFA) on a virtual private network (VPN) account, allowing hackers to exploit compromised credentials to breach the network.	The attack was facilitated by a lack of multifactor authentication (MFA) on a virtual private network (VPN) account, allowing hackers to exploit compromised credentials to breach the network.

The Toshiba Tec Group experienced a ransomware attack by the DarkSide hacking group, which threatened to compromise customer data and requested a ransom.	The attack occurred due to inadequate security measures that failed to prevent unauthorized access to their systems, allowing the hackers to exploit vulnerabilities.	Toshiba should enhance its cybersecurity by implementing robust security measures, including advanced threat detection systems, regular security audits, and employee training on recognizing phishing attempts and other attack vectors.
Raven Software had to remove a newly introduced pre-match lobby loadout selection feature in Call of Duty: Warzone due to significant bugs, which gave some players unfair advantages and disrupted gameplay.	The glitches arose from insufficient testing of the new feature, which failed to identify critical issues such as players spawning with customized loadouts and triggering an infinite Dead Silence effect.	Raven Software should implement more rigorous testing protocols, including extensive beta testing with diverse user groups, to identify and resolve potential issues before rolling out new features.
England's National Health Service (NHS) experienced a four-hour outage affecting both its app and website, preventing users from proving their COVID vaccination status and causing significant disruption for travelers.	The outage was likely due to system overload or failure in the centralized infrastructure, which could not handle the demand during a critical period.	The NHS should consider decentralizing its systems to improve resilience, along with implementing load testing and redundancy measures to ensure service continuity during high-demand periods
Tesla recalled nearly 12,000 vehicles due to a glitch in its Full-Self Driving beta software that caused false forward collision warnings, leading to sudden automatic emergency braking (AEB) and increased risk of rear-end collisions.	The issue stemmed from a communication error within the 10.3 Full-Self Driving (FSD) beta software, which triggered incorrect warnings and unnecessary braking	Tesla should enhance its software testing and validation processes, including robust simulation and real-world scenario testing, to catch potential glitches before updates are rolled out, ensuring vehicle safety and reliability.
The Log4j vulnerability has exposed millions of web servers to potential exploitation by hackers, posing a severe threat to	The issue arises from a flaw in the Log4j logging library, which allows attackers to execute arbitrary code by manipulating log messages,	Organizations should prioritize immediate patching of affected systems, implement comprehensive security

organizations worldwide due to its widespread use in critical systems	leading to potential malware installation and data breaches	audits, and enhance their monitoring for unusual activity, while also developing a long-term strategy that includes adopting a more proactive security framework to mitigate future vulnerabilities