Microsoft outage disrupts services worldwide

- *The outage caused numerous devices using the Windows operating systems to crash, with millions of users seeing the so-called 'blue screen of death' on their systems.*

Gulveen Aulakh

Published19 Jul 2024, 11:31 PM IST

The outage lasted hours and disrupted ground transport systems, flights, banking operations, stock exchanges, brokerages, hospitals, auto companies and systems that were using Microsoft services, globally.

New Delhi: A severe outage at Microsoft's cloud service Azure on Friday, caused by an update from cyber security firm CrowdStrike, created havoc across a wide spectrum of industries globally as well as in India.

The outage led to companies shifting to manual processes and also cancelling services in some cases. Things seemed to be veering towards normal by the end of the day, but uncertainty abounded even as Microsoft tried to assuage nerves and the Indian government spelt out steps taken to fix the issue.

The outage caused numerous devices using the Windows operating systems to crash, with millions of users seeing the so-called ‘blue screen of death’ on their systems.

The outage lasted hours and disrupted ground transport systems, flights, banking operations, stock exchanges, brokerages, hospitals, auto companies and systems that were using Microsoft services, globally.

The outage also impacted media, payment systems in different parts of the world, including Australia and the UK, 911 services across several states in the US, and services at London Stock Exchange and Sky News, which went off air.

Microsoft chief executive officer Satya Nadella said in a post on X, "Yesterday, CrowdStrike released an update that began impacting IT systems globally. We are aware of this issue and are working closely with CrowdStrike and across the industry to provide customers technical guidance and support to safely bring their systems back online."

India's IT minister Ashwini Vaishnaw said, “The reason for this outage has been identified and updates have been released to resolve the issue,” adding that the country's emergency response team Cert-in has also been roped in to handle the situation.

Flights Derailed in India

In India, the outage resulted in long queues at airports, flight delays and cancellations, causing inconvenience to passengers, and severely impacting critical systems used for flight operations, passenger check-in and baggage handling. Airlines shifted to manual or backup systems making it difficult for airline staff to ascertain passenger details and leading to delays across flights.

As per aviation analytics company Cirium, there were around 110,000 scheduled commercial flights globally on Friday, 19 July. As of 3:30 pm IST, 1,390 cancelled flights were cancelled and growing, Cirium said.

“For India, 3,652 flights scheduled originating from Indian destinations, with 56 cancellations so far. This does not include inbound flights to India,” Cirium said. A large number of flights, however, were delayed.

Airlines said they are prioritising operations to ensure flights take off with minimal delay. The civil aviation ministry said that it has implemented manual backup systems in collaboration with Airports Authority of India to maintain operational continuity.

The ministry also said that the terminal operations team is working closely with the airlines and the Central Industrial Security Force (CISF) to ensure minimal disruption and inconvenience to passengers. Additionally, the Directorate General of Civil Aviation (DGCA) is closely monitoring the situation with airlines to ensure all safety and procedural measures are in place.

From a manufacturing standpoint, India's leading car maker Maruti Suzuki told exchanges that its production and dispatch operations had temporarily halted, but it took remedial and precautionary measures and was able to resume operations later in the day. No material impact is expected from the incident, it said.

Financial Services Impact

Meanwhile, banking regulator Reserve Bank of India said about 10 banks saw minor disruptions and have been asked to remain alert.

“Our assessment shows that only 10 banks and NBFCs had minor disruptions which have either been resolved or are being resolved. Overall, the Indian financial sector in the Reserve Bank’s domain remains insulated from the global outage. The Reserve Bank has issued an Advisory today to its Regulated Entities for taking necessary steps to remain alert and ensure operational resilience and continuity,” RBI said in a statement.

While stock markets were not impacted due to the outage, some brokerage houses were impacted.

“Due to a global outage…our systems are affected. Our team is working closely with both of them to restore our systems as soon as possible," brokerage firm 5paisa said in a statement.

A dealer from a local brokerage house stated that only brokerages using Microsoft software were affected, and all brokerages using the cloud computing platform Azure would have experienced the issue. Analysts noted that brokerages were unable to access the data stored on the cloud drive.

Abhilash Pagaria, head of Nuvama Alternative and Quantitative Research, stated that the outage lasted two to three hours but was resolved thereafter. The glitch involved the system restarting repeatedly. However, he added that no trades were affected.

“NSE and NCL are working normal today,” spokesperson of the National Stock Exchange said.

Firms like Groww and Zerodha said they were not impacted.

Healthcare Impact

Services at hospitals like Max and Fortis were also disrupted with the outage impacting diagnostic and other patient services.

“Due to the outage, many of our software applications used for patient care and other processes were impacted," a spokesperson from Max Healthcare said, adding that its hospitals had to switch to manual processes to service patients as an alternative mechanism.

“After implementing the recovery process provided by Crowdstrike, our systems have fully restored, and we have resumed regular operations,” the spokesperson added.

Another hospital chain, Fortis, said in a statement, “At Fortis, we experienced a brief interruption in our diagnostic services, which was managed efficiently. Our systems continue to run normally, and we have conducted thorough checks to verify this."

Apollo said there was no impact in operations.

Government Intervention

Minister Vaishnaw added that the IT ministry was continually in touch with Microsoft, which in turn was actively working with impacted entities. “In addition, Cert-In is coordinating with chief information security officers of critical infrastructure entities. All impacted entities are working to bring up their systems. In many cases, systems are partially up.”

He added that Cert-In had issued a technical advisory. Cert-in refers to the Indian computer emergency response team, which is part of the ministry of electronics and information technology.

Cert-in's advisory said, “The issues occurred in the latest update of CrowdStrike and the changes have been reverted by the Crowd Strike Team.” It also suggested mitigation routes in case users were unable to stay online to receive the ‘Channel File Changes’.

Not a Security Scare

CrowdStrike, however, said that the widespread disruptions were not the result of a security incident or cyberattack.

CEO Kurtz posted on social media platform X that the company “is actively working with customers impacted by a defect found in a single content update for Windows hosts”. Mac and Linux devices or computers are not impacted.

Kurtz further said, “Today was not a security or cyber incident. Our customers remain fully protected. We understand the gravity of the situation and are deeply sorry for the inconvenience and disruption. We are working with all impacted customers to ensure that systems are back up and they can deliver the services their customers are counting on. As noted earlier, the issue has been identified and a fix has been deployed. There was an issue with a Falcon content update for Windows Hosts.”

Unprecedented Outage

Cybersecurity experts termed the scale of the impact as unprecedented.

Prominent security consultant Troy Hunt said “this will be the largest IT outage in history” and “this is basically what we were all worried about with Y2K, except it’s actually happened this time”.

Omer Grossman, chief information officer (CIO) at CyberArk said, “The current event appears that it will be one of the most significant cyber issues of 2024. The damage to business processes at the global level is dramatic.”

He added that since the endpoints or devices have crashed, they cannot be updated remotely and would have to resolved individually. The exercise would mean either repair or replacement of devices or laptops, which can take days.

This would also mean a large financial impact on businesses owing to loss of business as well as additional costs towards replacement of the impacted machines.

The range of reasons behind the outage ranges from human error—for instance, a developer who downloaded an update without sufficient quality control—to the complex and intriguing scenario of a deep cyberattack, prepared ahead of time and involving an attacker activating a “doomsday command” or “kill switch”, Grossman said.

“CrowdStrike's analysis and updates in the coming days will be of the utmost interest,” he said.

Dhiraj Gupta, chief technology officer of MFilterIt, a fraud detection and prevention firm, said that the outage exhibited the extent of how interlinked everyone has become and how it is becoming important for systems across own as well as vendors to be tracked.

“When many providers depend on a single provider, that provider in effect becomes a critical infrastructure provider. This may or may not be a result of a cyber security attack, but end result is of challenges on our day to day life irrespective,” he said.

Vishal Salvi, CEO, Quick Heal Technologies Limited, a cybersecurity company, said “We would like to assure that our customer base across the globe continues to remain safe and unaffected by this incident. It is our endeavour to ensure the highest safety and testing standards across our comprehensive suite of solutions.”

Salvi also said that the incident is not to be overlooked and highlights that no business is fully secure in today’s digital environment and things do go wrong.

“We urge the entire ecosystem to come together to prioritize proactive defense strategies and cybersecurity ‘Atamnirbharta’ to safeguard our digital infrastructure against evolving threats and incidents like these. In such an event, enterprises should have comprehensive contingency plans in place. These should include regular data backups, a robust disaster recovery strategy, and clear communication protocols to ensure minimal disruption,” said Salvi.