# European airports grapple with fallout as cyberattack disrupts key airline systems at Heathrow and beyond



Heathrow Airport, alongside several major European airports, experienced significant flight delays and cancellations following a cyberattack on September 19, 2025, which disrupted electronic check-in and baggage handling systems. The attack targeted the MUSE software provided by Collins Aerospace, a system used by multiple airlines to facilitate shared check-in desks and boarding gates. According to the airport’s initial communication, the disruption was described as a "technical issue," but further details revealed its cyber-related nature, prompting operational adjustments including manual check-in and boarding processes to mitigate passenger impact.

Brussels Airport reported some of the most severe consequences, cancelling nine flights and advising airlines to reduce departing flights by half between September 20 and September 22 to manage ongoing system issues. Passengers faced long queues and extended wait times as baggage tagging and check-in procedures reverted to manual methods. In contrast, Heathrow’s operations were reported to be less severely affected, with British Airways utilising backup systems to maintain service continuity, though most other airlines at the airport experienced disruptions. Berlin’s Brandenburg Airport also noted delays and longer waiting times due to the system outage.

The parent company of Collins Aerospace, RTX, acknowledged the cyber disruption and confirmed efforts to resolve the issue as swiftly as possible. They emphasised the impact was limited to electronic check-in and baggage drop-off systems, which could be alleviated through manual operations. Industry observers point to the attack exposing vulnerabilities in the aviation sector’s reliance on third-party digital infrastructure. Travel journalist Simon Calder told the BBC that disruptions at interconnected hubs like Heathrow could have cascading effects, affecting flight connections and the broader network.

Passengers conveyed the frustration caused by the delays and operational uncertainty. For instance, some reported lengthy queues exceeding two hours, with passengers being checked in manually over the phone, only to face boarding pass scanning issues at gates. Accessibility challenges were also highlighted, such as a passenger unable to secure necessary mobility assistance due to system outages.

Cybersecurity experts have speculated on the nature of the attack, with some suggesting it might be a ransomware incident—though the origin remains unclear. While there have been unfounded allegations linking the breach to Kremlin-sponsored hackers, the consensus among analysts is that recent cyberattacks on critical infrastructure are more commonly perpetrated by financially motivated criminal groups operating globally. Many known hacking groups are based in Russia or former Soviet states, though arrests worldwide suggest a diverse geography of cybercriminal activity, including actors from the UK and the US.

This incident follows other notable technological disruptions impacting UK airports in recent years, including border control system outages in 2024 that caused passport processing delays but were not attributed to cyberattacks. The recurring technological vulnerabilities and coordination complexities underline the importance of robust and resilient systems within the aviation industry to safeguard operational integrity and passenger experience against evolving cyber threats.

Heathrow has deployed additional staff to support check-in areas and advised passengers to verify flight statuses with their airlines before travelling, aiming to ease the disruption during this period. Transport Secretary Heidi Alexander confirmed government monitoring of the situation and efforts to receive regular updates on the unfolding event.

The broader European aviation network continues to manage the fallout from the cyberattack, underscoring the critical need for enhanced cybersecurity measures across the sector to prevent future incidents that can severely disrupt air travel and airport operations.

### 📌 Reference Map:

* Paragraph 1 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/), [[4]](https://www.scmp.com/news/world/europe/article/3326254/cyberattack-disrupts-european-airports-including-heathrow-berlin), [[6]](https://www.itv.com/news/2025-09-20/passengers-facing-another-day-of-disruption-after-check-in-system-cyber-attack)
* Paragraph 2 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/), [[2]](https://www.reuters.com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/), [[3]](https://apnews.com/article/29b6d890baf7ac3a22f0f2b2f169b890)
* Paragraph 3 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/), [[2]](https://www.reuters.com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/), [[4]](https://www.scmp.com/news/world/europe/article/3326254/cyberattack-disrupts-european-airports-including-heathrow-berlin)
* Paragraph 4 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/)
* Paragraph 5 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/)
* Paragraph 6 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/)
* Paragraph 7 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/), [[5]](https://www.reuters.com/world/uk/heathrow-airport-says-uk-border-force-experiencing-nationwide-issue-2024-05-07/)
* Paragraph 8 – [[1]](https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/), [[6]](https://www.itv.com/news/2025-09-20/passengers-facing-another-day-of-disruption-after-check-in-system-cyber-attack), [[7]](https://www.thenationalnews.com/business/aviation/2025/09/20/heathrow-and-european-airport-flight-delays-after-cyber-attack/)

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://cedirates.com/news/cyber-attack-causes-delays-at-heathrow-and-other-european-airports/> - Please view link - unable to able to access data
2. <https://www.reuters.com/en/cyberattack-causes-flight-delays-cancellations-brussels-airport-2025-09-20/> - A cyberattack on September 19, 2025, disrupted check-in and boarding systems at several major European airports, including Heathrow, Brussels, and Berlin. The attack targeted Collins Aerospace's MUSE software, leading to flight delays and cancellations. Brussels Airport advised airlines to cancel half of their scheduled departing flights on Sunday to manage ongoing disruptions. RTX, Collins Aerospace's parent company, acknowledged the issue and is working to resolve it. Passengers were advised to check flight statuses with airlines before traveling.
3. <https://apnews.com/article/29b6d890baf7ac3a22f0f2b2f169b890> - On September 20, 2025, a significant cyberattack disrupted check-in and boarding systems at major European airports, including Heathrow, Berlin's Brandenburg, and Brussels. The attack targeted Collins Aerospace's MUSE software, affecting multiple airlines. Brussels reported the greatest impact, with nine flights canceled and others delayed or rerouted. Heathrow and Berlin experienced minimal disruption. Experts suggested the attack could have been executed by sophisticated cybercriminals or state actors, highlighting vulnerabilities in the airline industry's reliance on centralized digital systems.
4. <https://www.scmp.com/news/world/europe/article/3326254/cyberattack-disrupts-european-airports-including-heathrow-berlin> - A cyberattack on September 19, 2025, targeted check-in and boarding systems at several major European airports, including Heathrow, Berlin, and Brussels. The attack rendered automated systems inoperable, necessitating manual check-in and boarding procedures. Collins Aerospace, the service provider, acknowledged the issue and is working to resolve it. Passengers were advised to check flight statuses with airlines before traveling. The incident underscores the vulnerability of critical infrastructure when relying on third-party suppliers.
5. <https://www.reuters.com/world/uk/heathrow-airport-says-uk-border-force-experiencing-nationwide-issue-2024-05-07/> - In May 2024, British airports experienced long queues due to a nationwide technical issue with the Border Force, causing delays in passport processing. The Home Office confirmed the outage was resolved and assured that border security had not been compromised, ruling out any cyber attack. Heathrow and Stansted airports reported their border control systems were operational again. This incident followed similar outages in May 2023 and an air traffic system disruption in August 2023.
6. <https://www.itv.com/news/2025-09-20/passengers-facing-another-day-of-disruption-after-check-in-system-cyber-attack> - Passengers faced disruptions at several European airports, including Heathrow, following a cyberattack on September 19, 2025, targeting a service provider for check-in and boarding systems. The attack led to manual check-in and boarding procedures, causing delays and cancellations. Heathrow advised passengers to check flight statuses before traveling. The incident highlights the vulnerability of critical infrastructure when relying on third-party suppliers.
7. <https://www.thenationalnews.com/business/aviation/2025/09/20/heathrow-and-european-airport-flight-delays-after-cyber-attack/> - Following a cyberattack on September 19, 2025, several European airports, including Heathrow, experienced flight delays and cancellations. The attack targeted Collins Aerospace's MUSE software, affecting multiple airlines. Passengers were advised to check flight statuses with airlines before traveling. The incident underscores the importance of cybersecurity in the aviation industry and the need for robust systems to prevent such disruptions.