CYBEREDBOARD BRIEFING

Five Outages, Six Days: Why the Systems Failed

What Microsoft, the FAA, JPMorgan Chase, the NSA and Apple disclosed about their November outages

November 2026

CyberEdBoard
powered by SMG

Five Outages, Six Days: Why the Systems Failed

What Microsoft, the FAA, JPMorgan Chase, the NSA and Apple disclosed about their November outages

When a New York Times reporter reached a recorded line for National Security Agency employees on the morning of Tuesday, November 17, the agency had declared a "code yellow" for the day shift at its Fort Meade, Maryland, headquarters, the middle level of a three-tier system. "Nonemergency personnel should begin staggered arrival no earlier than noon," the agency said in the recording. "Emergency personnel to report for duty as scheduled." NSA Net, the agency's classified internal network, was disrupted. Officials staggered arrivals to keep tens of thousands of personnel from signing in at the same time, a person familiar with the situation told Recorded Future News.

Apple's systems failed the same day. Its retail store systems went offline, and customers could not complete purchases, according to MacRumors. Employees lost AppleConnect, the company's internal sign-in system, people familiar with the matter told Bloomberg's Mark Gurman. Apple said an internal update had caused the outages.

Apple's was the fifth systems outage in six days. Microsoft has traced a disruption of many Microsoft 365 services, lasting nearly 24 hours, to a software defect. The Federal Aviation Administration has said it stopped departures nationwide for almost five hours. JPMorgan Chase has attributed a disruption to its banking services to a software bug. CNN and The New York Times each reported the NSA outage as the latest in this series, and Security Affairs said there was no evidence that the outages were connected.

In three of the five outages, a failure in one component spread beyond it. Microsoft has said that more than 80% of the servers on its Microsoft 365 networking gateway became unresponsive and that the failure spread globally. The FAA traced a flood of connection attempts to two sites, and the instability spread from Air Route Traffic Control Centers to several terminal radar approach controls, the agency said. A software bug in one JPMorgan Chase system delayed transactions at other banks and on Zelle, according to the bank and the Associated Press.

All five operators have attributed their outages to internal causes, and four have ruled out or found no indication of a cyberattack. Their accounts range from a dated root-cause report under a Microsoft executive's name to brief statements from Apple and the NSA that name a cause without naming the system that failed. The NSA said only that it had experienced "temporary degradation during scheduled routine maintenance"; sources who spoke to reporters linked the disruption to patching or software upgrades.

Operator	Dates	Duration	Stated cause	Source of the account
Microsoft 365	Nov. 12–13	Nearly 24 hours of active impact	A defect introduced in July, triggered by added load and reduced server capacity	Microsoft executive, on the record
FAA	Nov. 13	Ground stop of about 4 hours 45 minutes	Legacy equipment destabilized by a flood of connection attempts traced to two sites	FAA, on the record
JPMorgan Chase	Nov. 16	Not stated; restoration targeted for end of day	A software bug in an on-premise hardware system	Bank spokesman, on the record
NSA	Nov. 17	Not stated	Scheduled routine maintenance	NSA statement to Newsweek, on the record
Apple	Nov. 17	Not stated	An "internal update"	Apple statement to Bloomberg, on the record

Microsoft: a July defect, set off by a failover and missing capacity

Microsoft recorded active impact from 11:20 a.m. ET on November 12 until 11:10 a.m. ET on November 13 on the gateway serving many Microsoft 365 services, according to IBTimes UK. Charles Lamanna, Microsoft's executive vice president of Copilot, Agents and Platform, posted an abridged root-cause account on X on November 16, with fuller detail in the Microsoft 365 admin center.

Lamanna named three factors that combined, in a post Fox Business quoted. "First, a latent defect caused servers to become overwhelmed and unresponsive under certain load conditions," he wrote. The defect came from a change made in July specifically for the Microsoft 365 gateway servers, and the change had run worldwide for more than three months without problems. Microsoft's lab testing used a different mix of traffic and hardware, was weighted toward weaker machines, and missed a defect that affected newer machines with more cores more severely.

The second factor was load. About 15 hours before the outage, Teams traffic failed over from an alternative gateway to the primary one. The third was capacity: nearly 14% of the gateway's server capacity was already offline from an unrelated issue the previous day. Once the defect was triggered during peak U.S. business hours, more than 80% of the gateway's servers were unresponsive in less than two hours. A separate problem stopped network-partition safeguards from containing the failure, so it spread globally.

According to Microsoft, its rollback tools could not quickly reverse a months-old defect, and servers brought back online were overwhelmed by queued traffic. Microsoft engineers returned the connection-handling code to a previous stable state through an update, then restarted server groups and brought traffic back gradually. Teams, OneDrive, SharePoint and Office moved off the failing infrastructure and recovered sooner; Exchange Online could not make the same switch. Microsoft said there was no indication of cyber or malicious activity. It has said a final post-incident review will follow within five business days of full resolution, and its repair-item list targets November 20 for a full list of actions.

FAA: a flood of connections traced to two sites

The FAA issued a nationwide ground stop at approximately 3:30 p.m. ET on November 13 after what it called a technical problem, and air traffic resumed at 8:15 p.m., according to the agency's published questions and answers. "The FAA's legacy equipment became unstable when data began flooding the FAA FTI network, at a rate of 1,000 connection attempts every 4 to 5 seconds," the FAA states. Instability began at 17 of 22 Air Route Traffic Control Centers and spread to several terminal radar approach controls.

The FAA's initial investigation points to two locations: a radar site in Amarillo, Texas, and a radio communications site in El Dorado, Arkansas, where L3Harris, the FAA's network service provider, had been deploying a new router. L3Harris blocked both sites and the network stabilized. The FAA states that its upgrade and modernization work did not cause the outage. The FAA also says maintenance work was done midday instead of at night and that it will reevaluate when such work is scheduled. The agency has since disabled broadcasting on all of the new routers and on about 60 similar routers.

Some radio frequencies and radar feeds stayed up, so controllers could keep communicating with and tracking aircraft, and the FAA says it was not a full outage. About 3,500 aircraft landed safely, and the FAA says life-saving, law enforcement and military flights continued. Aircraft operators canceled about 12,462 flights, though the FAA says not all of those cancellations were directly caused by the ground stop. "Based on all available evidence, we have no indication that this was a cyberattack or an outside nefarious actor," the FAA states.

JPMorgan Chase: a software bug in an on-premise system, felt at other banks

Thousands of customers reported trouble at several major U.S. banks and with Zelle on Monday, November 16, after a technical issue at JPMorgan Chase, according to the Associated Press. Spokesman Joe Evangelisti attributed it to "a temporary issue related to a software bug in an on-premise hardware system" and said "it is not cyber-related." He said "This is not a systemic issue," and that other banks were affected only where they were transacting with Chase. Chase said it aimed to restore services by the end of Monday.

Bank of America and Citigroup said their own services were working. U.S. Bank said its systems were not directly affected, but that "clients attempting to send or receive Zelle payments with another financial institution may experience transaction delays." Early Warning Services, which owns Zelle, said "the Zelle network was fully operational."

NSA: routine maintenance, patching, and staggered sign-ins

The NSA's classified internal network, NSA Net, went down on Tuesday, November 17, according to six people who spoke to CNN. Two sources told CBS News the outage resulted from routine system patching, while adding that the precise circumstances remained unclear. Four of six people who spoke to Nextgov/FCW said it may be linked to a series of software upgrades on the network. One person told The New York Times the network had been unstable for weeks.

The NSA gave its account in a statement to Newsweek on the day of the outage, saying the agency "experienced temporary degradation during scheduled routine maintenance." It added, "While some internal systems were affected, mission/critical capabilities remain fully operational." The NSA did not name the systems affected or the maintenance involved.

One person told Recorded Future News the network was providing "intermittent service" and had not fully shut down. CBS sources said some work moved to other NSA facilities. Sources who spoke to CNN, CBS, the Times and Nextgov/FCW each saw no evidence or sign of a cyberattack.

Apple: an internal update reached customers, stores and staff

Apple listed iCloud Account & Sign In as slow or unavailable for all users from around 11:45 a.m. ET on Tuesday, November 17, a status-page entry BleepingComputer captured. People familiar with the matter told Bloomberg's Mark Gurman that the outage also took down AppleConnect, Apple's internal sign-in system, along with VPN access for remote employees, according to MacDailyNews. "When Apple sign in breaks, it isn't just one app," James Knight of Digital Warfare told Tom's Guide. Apple also listed Apple Business and Apple School Manager, its services for IT administrators who manage Apple devices, among the affected services, MacRumors noted.

Apple gave its account in a statement to Gurman, which MacRumors published at 2:14 p.m. ET: "Many of our systems are back up and running after an internal update caused some outages this morning. We're working to get the remaining systems online as soon as possible." Apple did not name the system the update changed, and it said the outage was not caused by a cyberattack. When 9to5Mac first reported the problems, Apple still listed the affected services as available on its System Status page.

All five operators named a cause; the detail varied

The five accounts differ in who gave them and how much they contain. Microsoft has posted root-cause detail in the Microsoft 365 admin center and an abridged version under an executive's name, with dates, percentages and named contributing factors. The FAA has published a question-and-answer page with a timeline, connection rates, the two sites and the vendor involved. JPMorgan Chase's account, given through a named spokesman, identifies a software bug in an on-premise hardware system and a same-day restoration target. Apple's account, a two-sentence statement given to Bloomberg, names an internal update as the cause. The NSA, in a statement to Newsweek, attributed the outage to scheduled routine maintenance and said its "mission/critical capabilities remain fully operational."

What comes next

Set aside the week's speculation and one pattern remains, and the government's top intelligence official has now stated it on the record. Director of National Intelligence Jay Clayton told the House Homeland Security Committee on November 18 that these were "separate service outages associated with maintenance and technical changes," ABC News reported. Four of the five trace back to a change made to the operator's own systems: a July fix at Microsoft, a router installation on the FAA's network, routine maintenance at the NSA and an internal update at Apple. Each was routine work of the kind every large enterprise schedules every week, and each disrupted systems far beyond its own scope.

CyberEdBoard is following four open threads. Microsoft's final post-incident review is due November 20. The FAA has paused installation of new Juniper routers while its investigation continues, and 13 Democratic senators have asked the FAA, L3Harris and Juniper for a technical briefing by November 23; L3Harris's copper-to-fiber program covers 3,648 routers, with about 400 installed so far, the senators said. The NSA and Apple have yet to say which systems failed. And Clayton has pointed at the process itself, "as you patch and upgrade your systems, taking them down and bringing them back up," which raises a question no operator has yet answered: whether the pace of change is outrunning the testing behind it.

None of the five outages had a confirmed adversary behind it. For security leaders, the exposure sits in their own change process.

Sources

- Recorded Future News: NSA Net, agency's classified internal network, faces unspecified disruptions
- MacRumors: Apple Blames Internal Update for Outage, Says It Wasn't a Cyberattack
- Security Affairs: Apple Services Disrupted as NSA Network Goes Down and Equinor Faces Cyberattack
- IBTimes UK: Microsoft Apologises for Massive Global Outage and Reveals Three Factors Behind the Widespread Disruption
- Fox Business: Microsoft reveals hidden bug behind global Outlook and Microsoft 365 outage
- Federal Aviation Administration: Nationwide Ground Stop: Questions and Answers
- Associated Press (via American Press): A technical issue at JPMorgan Chase triggers online banking delays for major US banks
- CNN: Exclusive: Highly classified US national security communications network goes down, sources say
- CBS News: NSA's classified internal network goes down, sources say
- Nextgov/FCW: Classified NSA communications network down, people familiar say
- Newsweek: NSA Down: Spokesperson Addresses Outage as Cyberattack Ruled Out
- BleepingComputer: Apple reports outages affecting iCloud Mail, AppleCare and more
- MacDailyNews: Apple blames internal update for iCloud outage, denies cyberattack
- Tom's Guide: Multiple Apple services were down including Apple Music and iCloud — live updates on sudden outage
- MacRumors: Apple is Down Today: Services, Stores, iPhones Unable to Activate
- 9to5Mac: iCloud, App Store, and other Apple services hit by ongoing outage
- ABC News: Trump administration continues to insist tech outages not cyberattacks
- Newsweek: FAA router rollout paused as senators press for safety testing
- Honolulu Star-Advertiser (Reuters): FAA pauses Juniper router installations after flight disruptions
- Airways Magazine: Senators' request to pause FAA Juniper router deployment
- The New York Times: Classified N.S.A. Network Goes Down, Causing Work Disruptions (link to be added)

This is a special briefing prepared for CyberEdBoard Members. We are offering it to you as an example of the quality and depth of our daily and weekly briefings. If you found this useful, consider applying for membership in our private global network of CISOs and CXOs. Find us at cyberedboard.io/