Eight outages. Six days. No attacker named.

Between November 12 and 17, email, air traffic, payroll, cloud, banking, an airline and a classified government network all went down. It was easy to assume the worst. So we went to the record: what each organization said happened, what's still unknown, and what a small or mid-sized business should take from it. Every claim below links to its source.

8 MAJOR OUTAGES

6 DAYS

3 BEGAN WITH PLANNED WORK

0 BLAMED ON ATTACKERS

---

12 THU
~24 HRS
[1] TECHRADAR ↗

Microsoft 365

Exchange Online began failing around 16:17 UTC, taking Outlook, Teams and Copilot down in at least 74 countries, with about 120,000 Downdetector reports in the U.S. alone. By hour 16 the problem was mostly isolated to Exchange; full service returned the morning of Nov 14. House staff said it cost them a day of legislative work.

STATED CAUSE A latent defect in its networking gateway servers, made worse by traffic changes and reduced capacity. Microsoft said there was no indication of a cyberattack.

TAKEAWAY If email is your only alerting channel, an email outage is also an alerting outage.

---

13 FRI
4H 25M
[2] CNBC ↗
[3] CNN ↗

FAA nationwide ground stop

The FAA halted every U.S. departure, the biggest stop to air travel since 9/11. Roughly 1,000 connection attempts every four to five seconds swamped its legacy telecom network, disrupting radio and radar feeds. About 12,462 flights were canceled that day, though not all because of the stop. CNN's sources say the FAA had little oversight of the contractor's work on site.

STATED CAUSE A router contractor L3Harris installed in El Dorado, Ark., during a copper-to-fiber upgrade. Officials see no sign of a cyberattack; engineers have reproduced the overload, but the root cause is still under investigation.

TAKEAWAY Your vendors' maintenance windows are your risk too. Ask who reviews and monitors their changes.

---

13 FRI
~18 HRS
[4] UC TODAY ↗

Workday

Employees at customers of a platform used by 11,500+ organizations couldn't clock in, check pay or finish benefits enrollment. Workday put its production tenants into maintenance Friday afternoon and restored service by Saturday morning; some employers extended enrollment deadlines.

STATED CAUSE During a disaster-recovery test, backup-site services connected to live production databases and left data inconsistent. Workday said it was not a cybersecurity incident.

TAKEAWAY Test your recovery plan, but isolate the test from production and have a rollback ready.

---

15 SUN
~3 HRS
[5] CSA ↗

AWS us-east-1

Starting at 3:05 a.m. Pacific on Sunday, sign-up, authentication and connectivity errors hit IAM Identity Center and about 11 other services in Amazon's busiest region.

STATED CAUSE Not disclosed. AWS hasn't said publicly what happened or whether an attack was ruled out.

TAKEAWAY When a provider won't say what happened, plan as if it could happen again.

Continued on page 2

16 MON
SAME DAY
[6] APPLESCOOP ↗

JPMorgan Chase and other banks

Chase customers saw delayed transactions and Zelle payments, with more than 20,000 Downdetector reports by mid-afternoon Eastern. Customers at other major banks reported trouble accessing accounts and processing transactions too.

STATED CAUSE A software bug in an on-premises hardware system. Chase said there was no sign of an attack.

TAKEAWAY Know your fallback for payroll and vendor payments before you need it.

16 MON
~90 MIN
[7] WIKIPEDIA ↗

United Airlines

Just before 5 p.m., United reported a widespread system outage. Crew apps, flight planning and weather tools needed for a safe takeoff went down, delaying departures. Flights already in the air and United Express weren't affected.

STATED CAUSE A software issue in internal systems; the pilots' union pointed to a weight-and-balance system. United said there was no sign of an attack.

TAKEAWAY If one system gates a critical step, it's a single point of failure. Find yours.

17 TUE
UNCONFIRMED
[8] CBS NEWS ↗

NSANet, the NSA's classified network

The network NSA staff use to share classified information went offline. The agency staggered arrival times so thousands of employees wouldn't log on at once; officials said mission-critical capabilities stayed operational. It's unclear how long the network was down.

STATED CAUSE Temporary degradation during scheduled routine maintenance; one source pointed to patching. Officials said there's no evidence of a cyberattack so far.

TAKEAWAY If patching can knock out the NSA's network, it can knock out yours. Stage updates and test first.

THE PATTERN

Nobody has shown these outages are connected, and we won't speculate. What the stated causes share is plainer: three began with planned work (an upgrade, a backup test, routine maintenance), three were software bugs, and one hasn't been explained.

OUR READ

Reading the published incident reports, our analysts' hunch is less exotic than a coordinated campaign: thinner teams, faster changes, and more trust in automation than in human review. An opinion, not a finding.

VSOC TIPS: DO THIS WEEK

Map your dependencies.
List the vendors you can't work without, and what you'd do if each one went dark for a day.

Have a plan B for comms.
Decide now how you'll reach staff, customers and your SOC without email or chat.

Watch for outage phishing.
Expect fake "service restored, sign in again" emails. No vendor needs your password to fix their outage. Send anything odd to the vSOC.

RECEIPTS

[1] TechRadar · Microsoft outage live coverage · Nov 13
[2] CNBC · Engineers replicate FAA network overload · Nov 18
[3] CNN · FAA had little contractor oversight · Nov 18
[4] UC Today · Workday's backup test · Nov 14
[5] Cloud Security Alliance · The November outage cluster
[6] AppleScoop · Every major outage of November 2026
[7] Wikipedia · November 2026 technology outages
[8] CBS News · NSA's classified network goes down · Nov 17

RADICL™

Causes as stated by each organization or reported by the linked source, as of Nov 18, 2026.