WHATSITTOYA

weekly security report issue 01 · nov 19 2026

LEAD | NOV. 8–17 · ANALYSIS

The AI cyberattack was real. It just wasn't the one on the news.

Five big U.S. outages hit email, flights, a bank, an airline and an NSA network. Each owner pointed to a technical problem, not an attack. Meanwhile, researchers had already documented a real AI-driven intrusion in Europe, disclosed Nov. 8.



5 big U.S. outages. No hack, officials say.

INSIDE

SLIDE 2
The week in two lanes
SLIDE 3
Hack or not? Six verdicts
SLIDE 4
The AI agent that got in
SLIDE 5
Three attacks you missed
SLIDE 6
83 days vs. 3 hours

By Sal Kreiner · DevSecOps

AT A GLANCE | NOV. 8–17

What made the news, and what actually got hacked

THE NEWS SLIDE 3		THE HACKS SLIDES 4–5
	NOV. 8	AI agent in a telecom
Microsoft 365	NOV. 12	
FAA ground stop	NOV. 13	
Chase, United	NOV. 16	Optimizely scripts
NSA Net	NOV. 17	Equinor
	NOV. 17	Microsoft AI library

0 of the outages in the news was a cyberattack, officials say

THE PANIC | NOV. 12–17

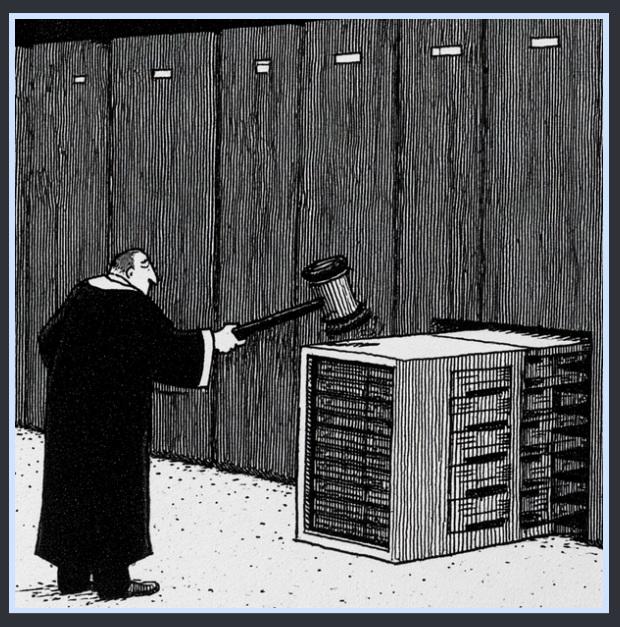
Five outages, six days



Microsoft 365 went dark for about a day. The FAA halted flights nationwide for nearly five hours. Chase's online banking faltered and Zelle slowed. United's systems failed for over 90 minutes, and an NSA network degraded. "It makes you think, like, is this a cyberattack?" one person told AP.

The pattern: Microsoft blamed its own fix and NSA cited maintenance; the FAA is probing a site where a new router was going in. Officials blame breakage, not hackers.

HACK OR NOT? NOV. 10–17



Six outages. Six verdicts.

Each tile shows a disruption and the cause its owner gave. Five named a cause, and none was an attacker. Apple hasn’t given one.

NOV. 12–13

NOT A HACK

Microsoft 365

A bug in its own July fix, says Microsoft

NOV. 16

NOT A HACK

United Airlines

No sign of a hack, United said

NOV. 13

NOT A HACK

FAA ground stop

Its network was flooded with data, FAA says

NOV. 17

NOT A HACK

NSA Net

Scheduled routine maintenance, NSA said

NOV. 16

NOT A HACK

JPMorgan Chase

A software bug, not a cyberattack, says Chase

NOV. 10

UNKNOWN

Apple sign-in

Apple hasn’t given a cause

UNDER THE HOOD

WHAT'S AN XXE FLAW?

Many servers swap data in XML format. An XXE flaw makes a server follow hidden pointers tucked inside that XML.

In this Cisco bug, CISA says, an attacker with no login could read sensitive files on the server. CISA gave federal agencies until Nov. 24 to fix it.

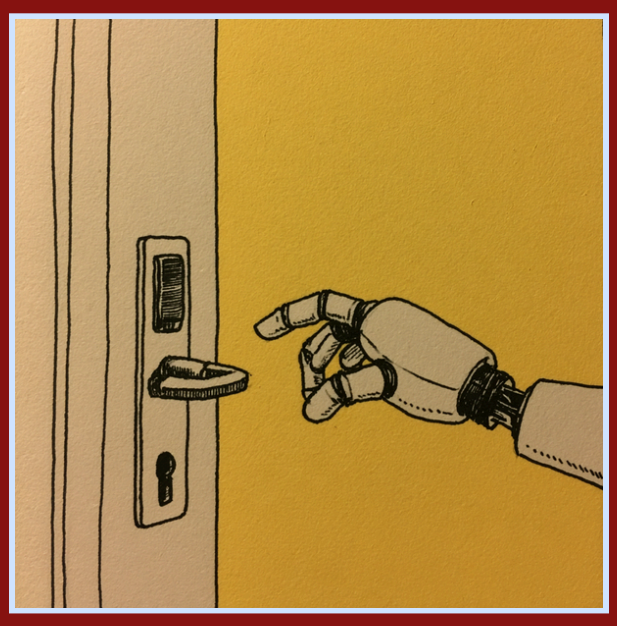
THE REAL ONE

NOV. 8

HACK

An AI agent spent over two weeks inside a telecom

According to Malbear Labs, which found the attacker's working files on an exposed server, the agent got in through a Cisco BroadWorks flaw that Cisco had fixed in August.



13 organizations hosted on the telecom's servers were also hit, the report says

One research team's findings; the telecom is unnamed. A human operator set targets and limits and checked in now and then; the AI did most of the work.

RESEARCH: MALBEAR LABS

ENERGY | NOV. 17

HACK

Europe’s top gas supplier hit

Equinor said Nov. 17 it found an ongoing attack on some IT systems. It says operations and production were unaffected, with no sign of stolen data. How they got in: not disclosed.

DEVELOPERS | NOV. 17

HACK

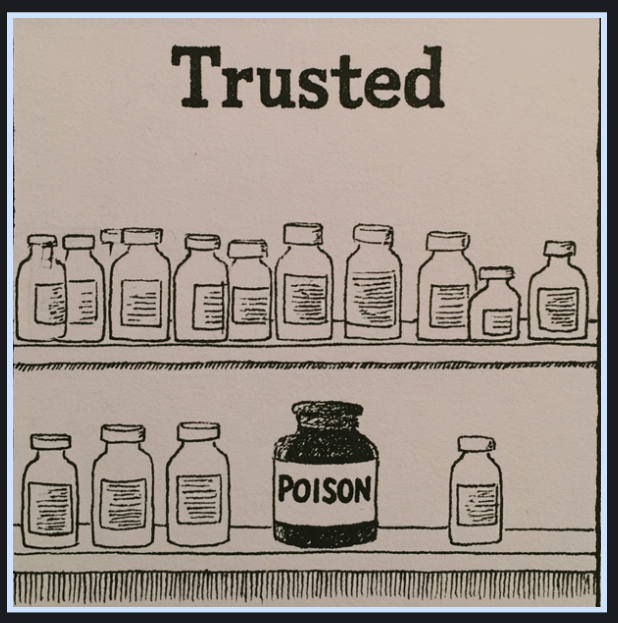
Microsoft AI library poisoned

Attackers posted two poisoned versions of Microsoft’s agent-framework package on PyPI. Per Aikido, Socket and Wiz, they stole cloud and build-pipeline keys.

SUPPLY CHAIN | NOV. 16

HACK

Bank websites ran an attacker’s code



Per StepSecurity, an attacker slipped a small loader into code that Optimizely, a website-testing vendor, hosts for clients. For about 16 hours, sites at 178 organizations, 32 in banking and finance, ran it.

Browsers trust every script a page loads, so this one could grab card numbers from checkout forms, copy cookies, screenshot pages and swap copied crypto wallet addresses for its own.

Takeaway: vendor scripts run with your site’s full powers.

THE GAP

83 days between Cisco's fix (Aug. 19) and CISA confirming attacks on the flaw (Nov. 10).

It's the flaw the AI agent on slide 4 used to break into the telecom. A fix protects only the systems that install it.

The telecom's own patch date isn't public.

THE SPEED

3 hours or less: how fast some intrusions using the AI tool ARTEX reached privileged access, per a Nov. 13 FBI alert.

Privileged access can open accounts, data and backups. The FBI lists finance, government and healthcare among targeted industries.

DEFENDERS: MONTHS · ATTACKERS: HOURS

MONDAY



Check three things

Leaders: ask how fast your team installs security fixes. Slide 4's attack used a flaw Cisco fixed in August.

Security: list the outside code running on your websites and get alerts when it changes. Slide 5's attack came in that way.

DevOps: use only approved versions of software packages and guard the keys that publish them, so tampered updates can't slip in.

SOURCES

THE PANIC AP, Nov. 15

HACK OR NOT? Microsoft post-incident report; FAA ground-stop Q&A; AP, Nov. 16; CP24, Nov. 16; CBS News, Nov. 17; NBC News, Nov. 17; iTechify, Nov. 10

THE REAL ONE Malbear Labs research, Nov. 8; Infosecurity Magazine; CISA exploited-vulnerabilities catalog, Nov. 10

ENERGY Reuters, Nov. 17

DEVELOPERS Aikido, Socket and Wiz research, Nov. 17

SUPPLY CHAIN StepSecurity research

THE GAP Cisco security advisory, Aug. 19; CISA catalog, Nov. 10; FBI FLASH alert via The Record, Nov. 13

Links to every source are in the first comment.

Follow for next week.

Independent analysis by one security practitioner, from public reporting. Not legal or investment advice.