THE DAILY TECH WIRE by Nuffield Consulting

Outages & Breaches: November 2025 in numbers

1 significant outage (1 critical) and 8 data breaches (3 critical) were logged in November 2025. The largest breach by records was Coupang (33.7M). The longest outage with a known duration was Cloudflare (5.8 hours). The most common outage cause was configuration change (1 of 1).

OUTAGES	CRITICAL OUTAGES	DOWNTIME TRACKED	BREACHES	CRITICAL BREACHES
1	1	6 h	8	3
▼ 3 vs October	wide impact	across 1 outage with a known duration	▲ 1 vs October	sensitive data at scale

RECORDS EXPOSED	FURTHER CLAIMED
36.7M	1.2M
confirmed or company-reported	attacker claims, unverified

OUTAGE CAUSES

Configuration change	1

NAMED ATTACKERS

Clop	2
Suspected insider	1
Qilin	1
ShinyHunters	1
Datacarry	1

MOST SIGNIFICANT INCIDENTS

30 Nov 2025	**Coupang breach exposes 33.7 million customers** Coupang · breach · Suspected insider · 33.7M records	CRITICAL
21 Nov 2025	**Gainsight apps abused to reach 200+ Salesforce customers** Gainsight / Salesforce · breach · ShinyHunters	CRITICAL
18 Nov 2025	**Cloudflare bot-management file knocks out a large slice of the web** Cloudflare · outage · Configuration change · 5.8 hours	CRITICAL

4 Nov 2025	**Swedish IT supplier breach exposes 1.5 million** Miljödata · breach · Datacarry · 1.5M records	CRITICAL
28 Nov 2025	**Asahi ransomware may have exposed 1.5 million customers** Asahi · breach · Qilin · 1.5M records	MAJOR
17 Nov 2025	**Logitech confirms data theft via third-party zero-day** Logitech · breach · Clop	MAJOR
13 Nov 2025	**Washington Post staff data stolen via Oracle EBS zero-day** The Washington Post · breach · Clop · 9.7K records	MAJOR
13 Nov 2025	**DoorDash customers' and dashers' data stolen** DoorDash · breach · Unknown	MAJOR

ALL 1 OUTAGE

18 Nov 2025	**Cloudflare bot-management file knocks out a large slice of the web** Cloudflare · outage · Configuration change · 5.8 hours	CRITICAL

ALL 8 DATA BREACHES

30 Nov 2025	**Coupang breach exposes 33.7 million customers** Coupang · breach · Suspected insider · 33.7M records	CRITICAL
28 Nov 2025	**Asahi ransomware may have exposed 1.5 million customers** Asahi · breach · Qilin · 1.5M records	MAJOR
21 Nov 2025	**Gainsight apps abused to reach 200+ Salesforce customers** Gainsight / Salesforce · breach · ShinyHunters	CRITICAL
17 Nov 2025	**Logitech confirms data theft via third-party zero-day** Logitech · breach · Clop	MAJOR
13 Nov 2025	**Washington Post staff data stolen via Oracle EBS zero-day** The Washington Post · breach · Clop · 9.7K records	MAJOR
13 Nov 2025	**DoorDash customers' and dashers' data stolen** DoorDash · breach · Unknown	MAJOR
4 Nov 2025	**Swedish IT supplier breach exposes 1.5 million** Miljödata · breach · Datacarry · 1.5M records	CRITICAL
1 Nov 2025	**Penn hacker claims data on 1.2 million donors and alumni** University of Pennsylvania · breach · Unknown · 1.2M claimed	MAJOR

2025 YEAR TO DATE

INCIDENTS YTD	OUTAGES YTD	BREACHES YTD	CRITICAL YTD	RECORDS EXPOSED YTD
127	**48**	**79**	**40**	**165M**
January to November 2025	significant outages	data breaches	outages and breaches	confirmed or company-reported

MONTH	OUTAGES	BREACHES	CRITICAL	RUNNING TOTAL
Jan	5	9	0	**14**
Feb	6	6	2	**26**
Mar	5	5	1	**36**
Apr	9	9	3	**54**
May	2	7	3	**63**
Jun	4	7	4	**74**
Jul	4	7	3	**85**
Aug	2	7	6	**94**
Sep	6	7	7	**107**
Oct	4	7	7	**118**
Nov	**1**	**8**	**4**	**127**
Total	**48**	**79**	**40**	**127**

CITE THIS

Nuffield Consulting, “Outages & Breaches: November 2025 in numbers”, The Daily Tech Wire,published November 2025. https://techwire.nuffieldconsulting.com/reports/2025-11/ (retrieved 15 Nov 2026).

The underlying data for every month is in the CSV download.

© 2026 Nuffield Consulting · Contact info@nuffieldconsulting.com

Compiled from public reporting and summarised in our own words. Every incident links to its original source. Severity: critical means wide impact, such as essential services disrupted or sensitive data exposed at scale; major means notable impact on one organisation's customers or a widely used service; minor is limited, brief or local. Outage status: ongoing (still disrupted at last report), partially restored, reported (state not yet confirmed), resolved, or post-mortem (cause explained by the

provider). "Claimed" marks figures from attackers that the organisation has not confirmed.