

INTELLIGENCE BRIEF

Z7 Weekly Cyber Friday Recap, November 21, 2026

Vendors were the story this week: n0n leaks tied to providers of Visa, Mastercard and JPMorgan Chase, plus Fireworks AI and Wellington IT. Five KEV entries need patching. Review vendor access first.

EDITION

Fall/Winter 2026/2027 Edition

TR-05 · Technology risk

PUBLISHED BY

Z7 Solutions LLC

Orlando, Florida

READ ONLINE

z7solutions.com

844-974-8669

01 At a Glance

STATUS

ONGOING RISK

Sources reviewed November 20, 2026. Several items below are investigations or extortion claims, and each is labeled as confirmed or claimed. [1]

HEADLINE NUMBERS

5

CISA KEV entries added November 17 and 18 [1]

149,346

People Uber notified after the Fireworks AI breach [4]

About 40

Irish credit unions with data exposed, per BleepingComputer [6]

11.25 million

Rakuten Securities accounts that may have had login IDs exposed [12]

KEY FACTS

REVIEWED

November 20, 2026

NEW KEV ENTRIES THIS WEEK

5 (Puppet Enterprise, Synology DSM, LiteLLM, Apache Axis, REDCap) [1]

DOMINANT PATTERN

Compromise of a third-party provider, not the named brand's own systems [2]

LARGEST CONFIRMED NOTICE

149,346 people notified by Uber after the Fireworks AI incident [4]

UNVERIFIED CLAIM TO WATCH

The Gentlemen listing for Nvidia, countdown to November 28 [10]

02 What Happened

Most of this week's headline incidents began at a supplier. Where a company has said something, this recap reports its statement. Where only a criminal group has spoken, it says claimed.

- n0n leaked data it claims belongs to JPMorgan Chase, Visa and Mastercard customers. Visa says the claims relate to a third-party provider in Asia Pacific, Chase says attackers reached marketing data held by vendors, and Mastercard says a third-party provider exposed a limited number of email addresses. None has named the provider. [2, 3]
- Uber notified 149,346 people that names, addresses, dates of birth and driver's license numbers were taken in a breach at its AI vendor Fireworks AI, and TechCrunch reports Fireworks confirmed the exposure of some customer data, with Notion saying about 1% of its customers were affected. [4, 5]
- Wellington IT, a software provider to Irish credit unions, is linked to a data exposure at roughly 40 credit unions; the company says its investigation is ongoing and the Irish minister called the notification delay not acceptable. [6, 7]
- The European Commission confirmed an AI generated cyber campaign that it detected on October 22, saying it found no evidence of a data breach affecting staff as a whole while its investigation continues. [8, 9]
- CISA added five exploited vulnerabilities to its KEV catalog on November 17 and 18: Perforce Puppet Enterprise, Synology DiskStation Manager, BerriAI LiteLLM, Apache Axis and Vanderbilt REDCap. [1]
- The Gentlemen ransomware group claims Nvidia on its leak site with a November 28 countdown and has shown no proof; Nvidia says it is investigating an incident that may have affected a third-party partner and has found no indication its own systems were affected. [10]

03 How It Works

01 Compromise the supplier, not the brand

The n0n, Fireworks AI and Wellington IT cases each trace back to an outside provider. [2, 3, 4, 6]

02 Abuse trusted vendor credentials

TechCrunch reports an attacker breached Fireworks AI's cloud provider to reach a Fireworks development system, and Uber was notified by its provider. Wellington IT reportedly saw an automated script using valid credentials to request payee records at scale. [4, 5, 6]

03 Exploit AI infrastructure and automation

CISA lists a LiteLLM flaw that allows code execution through a guardrails test endpoint. Separately, the European Commission confirmed that an AI tool was used in the campaign against it. [1, 8, 9]

04 Exploit NAS, research and legacy systems

CISA's new entries include Synology DSM, REDCap and an end-of-life-flagged Apache Axis library, all described as allowing remote code execution. Each is a system that often sits outside the core patch cycle. [1]

05 Certificates and test data as doors

The Puppet Enterprise flaw lets any client with a CA-signed agent certificate run code on the server, and becomes worse where certificate signing is automatic. Rakuten Securities said its breach related to its test-environment system. [1, 12]

04 Who Is at Risk

Organizations that depend on outside providers for software, analytics, AI or hosting carry the risk of that provider's security, whether or not they are the named victim.

- Financial institutions and credit unions that share member, marketing or payee data with software vendors. [3, 6]
- Teams that connected AI platforms, model hosts or gateways to production data and credentials. [1, 4]
- Universities, hospitals and research groups running REDCap, and any group running Synology, Puppet or Apache Axis. [1]
- Anyone who treats a vendor's compliance statement as a substitute for access limits and logging. [4, 6]

Sectors in scope: Financial services and card payments, Credit unions and banks that rely on outside software providers, Organizations using AI platforms, gateways and model hosting vendors, Public sector bodies and research institutions, Healthcare, schools and universities running REDCap or Apache Axis.

05 What Changed Since the Last Edition

EACH CHANGE WITH ITS SOURCE

01 November 18: CISA added CVE-2024-10441 (Synology DSM), CVE-2026-40217 (BerriAI LiteLLM), CVE-2026-90436 (Apache Axis) and CVE-2026-90817 (REDCap) to KEV. Federal due dates are November 21 for Synology, Axis and REDCap and December 2 for LiteLLM.

SOURCE 1

02 November 17: CISA added CVE-2026-115731 (Perforce Puppet Enterprise), with a December 1 federal due date. CISA's description says an agent certificate holder can execute code on the Puppet Server.

SOURCE 1

03 November 16 and 20: n0n leaked data it said came from Chase, Visa and Mastercard programs, and the three companies each pointed to a third-party provider in statements reported November 20. Chase said the matter has nothing to do with problems some customers saw earlier in the week.

SOURCE 2

04 November 16: Uber's notice count reached 149,346 people for the Fireworks AI breach, with Fireworks attributing the breach to a financially motivated cybercriminal group. Uber did not say how many were drivers.

SOURCE 4

05 November 18 and 19: Wellington IT's chief executive said the investigation is ongoing. The firm reportedly lacked activity logs that specify which member data was taken, so the number of people affected is unknown.

SOURCE 6

06 November 16: the US Justice Department announced that Roman Khlynovskiy, a Kazakh national, was extradited from Italy and appeared in federal court in Knoxville, Tennessee. Prosecutors allege he belonged to the 8-Digits Team, affiliated with INC and Lynx ransomware. He is presumed innocent.

SOURCE 11

07 November 17 and 18: Rakuten Securities said up to 11.25 million accounts may have had login IDs and client-specific codes exposed, and up to 4.47 million may have had personal data and assets exposed, in a breach of its test-environment system. The company said credentials for logging in and trading were not compromised.

SOURCE 12

08 November 18: the Hesse data protection commissioner announced an inquiry into whether Deutsche Bank promptly notified individuals after a whistleblower leak of more than 15 million internal records. The bank says its testing found no account information, login credentials or payment data was accessed.

SOURCE 13

06 What to Do Now

IN PRIORITY ORDER, HIGHEST IMPACT FIRST

01 DO FIRST **Patch or isolate Synology DSM, REDCap, Apache Axis, Puppet Enterprise and LiteLLM by name, starting with anything reachable from the internet.**

All five are now in CISA's KEV catalog with remote code execution described, and three had a federal due date of November 21. [1]

02 **Block or restrict the LiteLLM guardrails test endpoint and put AI gateways behind authentication and network limits.**

The KEV entry describes remote code execution through the /guardrails/test_custom_code URI. [1]

03 **Confirm your Puppet certificate authority does not auto-sign agent requests without strong verification.**

CISA's description says automatic signing lets an unauthenticated network attacker obtain a valid certificate and exploit the flaw. [1]

04 **List every vendor that holds your data or credentials, then remove access you do not need and rotate any shared secrets.**

The week's largest incidents began at suppliers, and Uber's data was taken in a breach at its vendor Fireworks AI. [3, 4]

05 **Require vendors to keep detailed activity logs and to notify you of incidents within a contractual window.**

Wellington IT reportedly lacked logs showing which data was taken, and the Irish minister called the disclosure delay not acceptable. [6, 7]

06 **Keep customer data out of test and development systems, or mask it before use.**

Rakuten Securities said its breach related to its test-environment system. [12]

07 **Treat leak-site claims as a trigger for verification, not as proof: ask suppliers directly and check your own logs.**

Nvidia has found no indication its own systems were affected, and n0n's claims name companies that point to third parties. [2, 10]

08 **Prepare notification contacts and a response plan for an incident at a supplier, including an AI vendor.**

Uber's notice count reached 149,346 people after the breach at its supplier. [4]

07 Sources

[1] **Known Exploited Vulnerabilities Catalog, version 2026.11.18** CISA · November 18, 2026. https://raw.githubusercontent.com/cisagov/kev-data/develop/known_exploited_vulnerabilities.json

[2] **JPMorgan, Visa, Mastercard cite third-party incidents amid data leak** SecurityWeek · November 20, 2026. https://www.securityweek.com/jpmorgan-visa-mastercard-cite-third-party-incidents-amid-data-leak/

[3] **Vendor data breach exposes Chase, Visa, Mastercard customer info** BleepingComputer · November 20, 2026. https://bleepingcomputer.com/news/security/vendor-data-breach-exposes-chase-visa-mastercard-customer-info

[4] **Uber confirms hackers stole thousands of drivers' license information in data breach** TechCrunch · Published November 13, updated November 16, 2026. https://techcrunch.com/2026/11/16/uber-confirms-hackers-stole-thousands-of-drivers-license-information-in-data-breach/

[5] **Fireworks AI data breach affecting Notion** TechCrunch · November 12, 2026. https://techcrunch.com/?p=3187828

[6] **Data breach impacts 40 Irish credit unions in reported IT provider hack** BleepingComputer · November 18, 2026, updated November 19. https://www.bleepingcomputer.com/news/security/data-breach-impacts-40-irish-credit-unions-in-reported-it-provider-hack/

[7] **Credit union data breach: Minister concerned over delay in disclosing cyberattack** The Irish Times · November 18, 2026. https://www.irishtimes.com/crime-law/2026/11/18/credit-union-data-breach-minister-concerned-over-delay-in-disclosing-cyberattack/

[8] **European Commission confirms AI-assisted cyberattack disrupted services** SecurityWeek · November 20, 2026. https://www.securityweek.com/european-commission-confirms-ai-assisted-cyberattack-disrupted-services/

[9] **European Commission confirms AI-generated cyberattack using a publicly available tool** Help Net Security · November 20, 2026. https://www.helpnetsecurity.com/2026/11/20/european-commission-ai-generated-cyberattack-publicly-available-tool/

[10] **NVIDIA investigating Gentlemen ransomware breach claims** BleepingComputer · November 19, 2026. https://www.bleepingcomputer.com/news/security/nvidia-investigating-gentlemen-ransomware-breach-claims/

[11] **Alleged member of 8-Digits Team ransomware group extradited from Italy** U.S. Department of Justice · November 16, 2026. https://www.justice.gov/opa/pr/alleged-member-8-digits-team-ransomware-group-extradited-italy-role-major-data-extortion

[12] **Rakuten Bank shares tank as securities arm faces data breach** The Star · November 18, 2026. https://www.thestar.com.my/business/business-news/2026/11/18/rakuten-bank-shares-tank-as-securities-arm-faces-data-breach

[13] **Data watchdog probes massive Deutsche Bank leak of 15m files** Euronews · November 18, 2026. https://www.euronews.com/2026/11/18/data-watchdog-probes-massive-deutsche-bank-leak-of-15m-files

NEXT STEP

What does this mean for your security?

Bring your questions about Week of November 14 to 20, 2026, your environment and the controls you rely on. Talk through the most useful next step with Z7 Solutions LLC.

01 / Exposure

Bring one question about how this threat could affect your environment.

02 / Priorities

Bring your current safeguards, open gaps and budget questions.

ALSO IN THIS EDITION

- Post-quantum deadlines set, attack estimates fall
  More from the edition · z7solutions.com/z7-cyber/quantum-era/
- LiteLLM and Puppet flaws put control planes at risk
  More from the edition · z7solutions.com/z7-cyber/ai-gateway-exploitation-litellm/
- November 2026 Threat Watch
  More from the edition · z7solutions.com/z7-cyber/november-2026-threat-watch/

CALL 844-974-8669

EMAIL sales@z7solutions.com

BOOK A SECURITY CONVERSATION — Book a Security Conversation ↗

Z7 Solutions™, Z7-Claw™ and Z7-Guard™ are trademarks of Z7 Solutions LLC.