It's Probably Nothing
by Sierra Echo Charlie

EDITION 36 / 26 NOVEMBER 2026

Juniper flaw exploited, NZ reported losses double

RNZ investigates disrupted systems, and Bendigo Bank gets an A$8m penalty.

5 stories / Listen online - 3:19

THE TAKEAWAY

The Juniper Session Smart flaw we covered in October is now on CISA's known-exploited list, and the agency is asking for forensic triage, not just a patch. Closer to home, NZ's latest cyber figures show a jump in reports and an even bigger jump in reported losses.

01 / THE BRIEF

CISA confirms exploitation of Juniper Session Smart flaw

CISA added CVE-2026-103406 to its Known Exploited Vulnerabilities catalogue on 25 November. When we covered it on 30 October, Juniper hadn't reported malicious exploitation. The entry names Session Smart Conductor and Session Smart Router and says the remote command-injection flaw can give an attacker root access. It doesn't specify affected builds, and ransomware use is unknown.

CISA calls for forensic triage and gives covered US federal agencies until 28 November. That deadline isn't local, but the distinction matters: patching closes the hole; it doesn't tell you whether someone already got in.

WORTH ASKING

Check Juniper's bulletin for your builds. If affected gear was exposed, treat it as a triage job as well as a patch job.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

Juniper Session Smart security bulletin - Primary source

02 / THE BRIEF

NZ incident reports hit a two-year high

NCSC received 1,694 reports in July-September, up from 1,129 the previous quarter. The number requiring specialist technical support rose from 92 to 179. Phishing and credential harvesting remained the biggest category, with 511 reports, up 56%. Reported direct losses rose 118%, from NZ$2.7 million to NZ$5.9 million. That's what people reported to NCSC, not an estimate of what the country lost.

SOURCES

Cyber security incidents hit highest level in two years and financial losses surge - Primary source

AI blamed for cyber security breaches surging - Reporting / context

03 / THE BRIEF

GeoServer probes reported; fixes shipped in October

SecurityWeek reports that watchTowr saw probes targeting CVE-2026-120705 and CVE-2026-129243, two flaws GeoServer describes as parts of a larger chain that can lead to remote code execution. The observed activity didn't establish that anyone got code running. The advisory is new this week; the fixes aren't.

WORTH ASKING

Put internet-facing instances first in the upgrade queue. GeoServer recommends 3.0.2, 2.28.6 or 2.27.7, depending on your branch.

SOURCES

GeoServer CVE-2026-129245 FAQ - Primary source

GeoServer Security Update - November 2026 - Primary source

Two Newly Disclosed GeoServer Vulnerabilities Under Attack - Reporting / context

GeoServer security advisory (AV26-1207) - Primary source

GeoServer Flaws Exploited as Researchers Disclose Unauthenticated RCE Chain - Reporting / context

04 / THE BRIEF

RNZ investigates possible breach after staff lose access

RNZ says its technical staff detected unusual activity in one system, took steps to contain it and notified NCSC. Some staff couldn't access Wi-Fi, editorial systems or the VPN on Wednesday morning. RNZ hasn't established whether data was exposed, who was behind the activity or whether there's any link to the Allied Media attack.

SOURCES

RNZ investigating potential cyber breach - Primary source

25 Nov: Update on cyber attack - Primary source

05 / THE BRIEF

Bendigo Bank ordered to pay A$8 million

A catch-up from 24 November: APRA says Australia's Federal Court ordered Bendigo and Adelaide Bank to pay A$8 million after the bank admitted breaching its accountability obligations. The 2023 incident involved about A$490,000 in unauthorised transactions across 87 customers, whom the bank reimbursed.

In APRA's account, the court's findings went beyond customer authentication: they covered systematic control testing and who was accountable for Alliance Bank's IT operations.

SOURCES

APRA secures $8 million penalty against Bendigo and Adelaide Bank over cyber incident - Primary source

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.