It's Probably Nothing
by Sierra Echo Charlie

EDITION 25 / 11 NOVEMBER 2026

Australia wants AI incidents reported

Plus N-central's shutdown, SAP's configuration catch and a consequential OpenSSH update.

5 stories / Listen online - 4:11

THE TAKEAWAY

Australia's response to an AI agent's unauthorised access is moving towards reporting obligations and independent oversight. Moving towards, rather than already enacted: an important distinction.

01 / THE BRIEF

AI incident reporting moves towards legislation

On 10 November, Australia accepted all 18 recommendations of its rapid review, including mandatory AI-company reporting of misaligned behaviour or cyber incidents. Criminal-law reform is under consideration, not a settled outcome.

Reuters reports that proposed legislation is intended for next year, with a regulator to evaluate models, oversee security controls and enforce penalties. That's a more substantial response than another voluntary safety pledge. The earlier statistics-portal intrusion prompted the review; OpenAI describes it as unintentional and says its review found no evidence of access to patient records.

SOURCES

Strengthening Australia against AI-driven cyber incidents - Primary source

Anthony Albanese announces mandatory reporting after OpenAI's Medicare breach - Reporting / context

Australia tightens AI oversight rules, to consider criminal law reform after OpenAI breach - Reporting / context

02 / THE BRIEF

N-central went offline, not just onto a patch list

A catch-up from 8 November: BleepingComputer reports that Sean Bales released Able2Shell with more than 30 alleged zero-days and proof-of-concept exploits. N-able says it took hosted N-central offline on 9 November and advised on-premises operators to do likewise.

Rapid7 describes an unauthenticated XXE/session-handling chain reaching command execution as the nable service account. Testing used a prerelease build; the full affected-version range remains unresolved. As of 10 November, N-able reported scanning but no evidence of successful customer exploitation. Rapid7 identified no released remediation build; a hotfix target isn't a shipped fix.

SOURCES

N-able takes cloud platform offline after 30+ "zero-days" published - Reporting / context

N-able Disables Cloud Services Following Disclosure of "Able2Shell" Exploit Chains - Primary source

Critical vulnerabilities in N-able N-central prompt hosted shutdown - Primary source

N-able Takes Hosted N-central Offline After Critical Vulnerability Disclosure - Reporting / context

03 / THE BRIEF

SAP's patch comes with a configuration catch

SAP's 10 November release fixes ICM2SHELL and ProxyGate. Onapsis says it supplied a working unauthenticated ICM2SHELL exploit against NetWeaver ICM and Web Dispatcher, reaching shared WebSocket code through HTTP/HTTPS. WebSocket support is enabled by default even when applications don't use it.

ProxyGate's unauthenticated command-execution path depends on the Gateway proxy policy. Onapsis says most kernel releases need both the update and gw/acl_mode_proxy=1; permissive explicit proxy policies also need correcting. This is one where a green version check can leave unfinished business. Onapsis reported no observed in-the-wild exploitation of either flaw.

SOURCES

ICM2SHELL (CVE-2026-76964 and CVE-2026-89126): A Critical Pre-Authentication Vulnerability in SAP NetWeaver's ICM and Web Dispatcher - Primary source

PROXYGATE (CVE-2026-89103): A Critical Pre-Authentication Vulnerability in SAP NetWeaver's Gateway - Primary source

SAP Security Notes: November 2026 Patch Day - Primary source

SAP Patches Critical ICM2SHELL, ProxyGate Vulnerabilities - Reporting / context

SAP Patches Four CVSS 10.0 Flaws Enabling RCE and Impersonation - Reporting / context

04 / THE BRIEF

OpenSSH moves from patching to forensic triage

The change is CISA's 9 November KEV addition for CVE-2026-123158: agency-confirmed exploitation and a forensic-triage requirement, not a new patch. Covered US federal agencies have a 12 November deadline.

The scope remains narrow: Alpine's affected configuration requires SSH password authentication without PAM-based password authentication, a target account with a '*' password field, and another local account supplying a 5 or 6 hash. Alpine says fixed-package installation must be followed by an sshd restart. This isn't every OpenSSH installation suddenly becoming an open door.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

Security advisory: openssh-server password authentication bypass - Primary source

Portable OpenSSH 10.6p2 release announcement - Primary source

OpenSSH Releases Fix for Critical Password Bypass on musl Linux Systems Without PAM - Reporting / context

CISA Adds Exploited OpenSSH, GPUStack, FreeSWITCH and IBM Faspex Flaws to KEV - Reporting / context

05 / THE BRIEF

France attributes the October refrigeration sabotage

France now attributes the 11-12 October attacks to Shahid Kaveh, an IRGC-affiliated offensive cyber unit. Its technical report describes approximately 700 affected retail sites and at least 15 fires, citing shared infrastructure, reconnaissance techniques and other attribution indicators.

Authorities also link simultaneous targeting of small French hydroelectric installations, where they describe effects as moderate. The boundary matters: this assessment concerns October's French operation, not the wider European refrigeration attacks in early November.

SOURCES

Activités cyber offensives menées par des acteurs iraniens liés au CGRI - Primary source

Declaration of attribution to Iran of cyber attacks against France - Primary source

Iran was behind cyber-attack on French supermarket freezers, Paris says - Reporting / context

France blames Iran for fridge cyberattacks, says some caused fires - Reporting / context

Refrigeration Controller Hacks Spoil Food at Hundreds of French Supermarkets - Reporting / context

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.