It's Probably Nothing
by Sierra Echo Charlie

EDITION 29 / 17 NOVEMBER 2026

A TCP race that takes the host down with it

NoisyTCP's uneven crash timings, Coles' disclosure and a cloud key that outlived its job.

5 stories / Listen online - 3:59

THE TAKEAWAY

A containerised web server is an awkward place to discover a host-killing kernel bug. Today's Linux research has that consequence, with some important qualifications.

01 / THE BRIEF

NoisyTCP: reachable service, host-level crash

Hyunwoo Kim's newly published NoisyTCP advisory describes a pre-authentication TCP race, CVE-2026-99288, that causes a kernel panic. In the researcher's tests, triggering it through a containerised web server also brought down the host.

The timing is worth reading past the headline: default Nginx, Apache and SSH services on QEMU/KVM guests crashed in approximately five seconds to two minutes. A quiet bare-metal Nginx server took approximately 14 hours, despite target-specific tuning. Exploitation requires at least two RX queues or receive packet steering across multiple CPUs.

The advisory identifies a 3 November kernel fix; distribution packages weren't verified here. This is demonstrated denial of service, not demonstrated code execution, and the advisory establishes no real-world exploitation.

SOURCES

NoisyTCP: Linux Kernel TCP Pre-auth Remote Corruption (CVE-2026-99288) - Primary source

02 / THE BRIEF

Coles discloses an incident, not a settled data assessment

Coles disclosed a cyber security investigation on 16 November and says it's working with the ACSC and external specialists to contain and secure its IT environment.

The company says it hasn't identified evidence that customer, employee or supplier data was compromised or removed. That's an interim finding, not a clean bill of health. Stores and online shopping remain operational, according to Coles. It separately acknowledged limited Liquorland click-and-collect problems without establishing their cause.

SOURCES

Coles Investigating Cyber Security Incident - Primary source

Updates from Coles Group - Primary source

Supermarket group Coles investigates cybersecurity incident but provides little detail - Reporting / context

03 / THE BRIEF

Barracuda's expired engagement left a working key

A catch-up from Barracuda's 10 November disclosure, separate from its ESG appliance flaws: the company says an attacker entered its cloud environment using a valid key supplied to an AI vendor and never retired after the engagement ended. Its 13 November update traced the exposure to a configuration file in the supplier's GitHub repository following compromise of that supplier's development environment.

Barracuda describes secrets leading into source-code and Kubernetes systems, including build workflows made to print encoded secrets into logs. It found no direct evidence of access to customer integration credentials, but insufficient logging means it can't rule that out.

WORTH ASKING

Notified Managed XDR Cloud and Monitored Endpoint integration customers were told to revoke and recreate credentials and review connected-system activity from 1 November.

SOURCES

Barracuda XDR Integration Credentials - Primary source

Forty-four hours: Anatomy of a machine-speed intrusion - Primary source

Attackers Used Artex AI Framework to Breach Barracuda Cloud Accounts - Reporting / context

04 / THE BRIEF

PostgreSQL object privileges can become OS execution

Another catch-up: PostgreSQL's 12 November security release fixes CVE-2026-6460, allowing an object creator to execute code as the operating-system account running PostgreSQL through type confusion, primarily involving ALTER ... SET DATA TYPE.

That's a database-to-OS boundary crossing, not unauthenticated access or automatic root. Fixed versions are 18.7, 17.12, 16.16, 15.20 and 14.25. Version 14 also stopped receiving fixes on 12 November.

SOURCES

CVE-2026-6460: PostgreSQL type confusion after ALTER ... SET DATA TYPE executes arbitrary code - Primary source

PostgreSQL: The world's most advanced open source database - Primary source

PostgreSQL Patches 52 Vulnerabilities, Including Code Execution and Authorization Bypasses - Reporting / context

05 / THE BRIEF

N-central HF3 starts rolling out, with boundaries

N-able's HF3 moved from validation into phased hosted deployment on 16 November, with EMEA started. That's progress, not an all-clear: global completion and on-premises availability weren't confirmed before cutoff. Hosted environments already had Legacy API protections; HF3 is intended to remove that access permanently alongside authentication and communications changes.

SOURCES

Status Dashboard - Primary source

N-able Vulnerability Remediation Update - Primary source

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

N-able Takes Hosted N-central Offline After Critical Vulnerability Disclosure - 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.