It's Probably Nothing
by Sierra Echo Charlie

EDITION 23 / 9 NOVEMBER 2026

The agent found a TODO. There goes the afternoon.

Google measures coding-agent detours, while SonicWall's SAML bypass lands in KEV.

5 stories / Listen online - 4:03

THE TAKEAWAY

A code comment doesn't need to be malicious to send an agent off-task. Google has put some numbers on that.

01 / THE BRIEF

Your TODO list is now the agent's side quest

Google's internal study found agents acted on bug references in 6% of encounters with inline TODO or FIXME references; 83% of those follow-up sessions were unprompted. Among detours into still-open bugs, 39% involved editing code outside the requested task.

After controlling for listed developer and task characteristics, Google associated unprompted detours with 77% more tokens and 105% more waiting time. This is observational research, not a causal experiment or a demonstrated attack. Still, ordinary repository clutter appears quite capable of generating its own scope creep.

SOURCES

Agent Distraction - Primary source

02 / THE BRIEF

SonicWall's SAML boundary has an alternative entrance

CISA added CVE-2026-19868 to KEV on 6 November, confirming active exploitation. SonicWall's CVE record says valid credentials for an alternative authentication method may bypass SAML controls, potentially including SAML-enforced MFA. This isn't passwordless access to every firewall: SecurityWeek reports that SAML login must be enabled on the SSL VPN service.

SonicWall's quoted wording is more cautious, referring to potential exploitation; neither it nor CISA supplies attack dates, actors or victims.

WORTH ASKING

For affected deployments, SecurityWeek reports fixes in SonicOS 7.3.4-7013 and 8.2.3-8015, with no workaround.

SOURCES

CISA Catalog of Known Exploited Vulnerabilities - Primary source

CISA Adds One Known Exploited Vulnerability to Catalog - Primary source

CVE-2026-19868 - Primary source

SonicWall Patches Exploited SonicOS Vulnerability That Weakens VPN Logins - Reporting / context

SonicWall SonicOS SSLVPN Flaw Exploited to Bypass SAML Authentication Controls - Reporting / context

03 / THE BRIEF

An error value that passes the password check

An earlier development worth catching up on: OpenSSH released 10.6p2 on 5 November for a password-authentication bypass on musl Linux systems without PAM.

Alpine documents the peculiar collision: a 257-1024-byte password makes musl crypt() return '*', matching a target account's stored '*' field. Exploitation requires password authentication enabled and another local account supplying a 5 or 6 hash.

Alpine says some official tiny-cloud images can become exploitable after a qualifying hash is added, allowing login as alpine and root elevation through passwordless doas. PAM-enabled systems, PasswordAuthentication no and containers without sshd fall outside its affected configurations.

WORTH ASKING

Alpine provides fixed packages and says sshd must be restarted; disabling password authentication and restarting is its interim mitigation.

SOURCES

Portable OpenSSH 10.6p2 release announcement - Primary source

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

"sshole": password authentication bypass: OpenSSH + musl libc - Reporting / context

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

04 / THE BRIEF

Arkéa's own account, not its customers'

Also catching up: Crédit Mutuel Arkéa disclosed on 4 November that attackers used an unnamed supplier's platform to make transfers from the bank's own account to other banks.

Asked about €118 million, the bank confirmed only the order of magnitude: some funds were blocked, and a final amount was premature. It says customer assets were unaffected, although precautionary suspensions delayed transfers. That reassurance concerns assets, not a completed assessment of customer-data exposure.

SOURCES

Additional Information Following the Cyberattack on Crédit Mutuel Arkéa - Primary source

Crédit Mutuel Arkéa annonce avoir été victime d'une cyberattaque - Primary source

Hackers steal about 100 million euros from French lender Credit Mutuel Arkea in rare bank cyberattack - Reporting / context

Crédit Mutuel Arkéa Hit by Third-Party Breach and Estimated €118 Million Theft - Reporting / context

05 / THE BRIEF

Marketing data is still customer data

ABC reports Who Gives A Crap disclosed exposure at a US-based marketing software supplier. The company says names, contact details, mailing addresses and total spend were involved, but not payment details, order details or passwords; customer accounts weren't directly accessed.

It doesn't know whether information was copied or downloaded and reports no evidence of misuse so far. Total spend is a useful reminder that a marketing dataset can reveal more than where to send the next email.

SOURCES

Who Gives A Crap confirms customer data exposed in software breach - Reporting / context

Who Gives A Crap customers caught up in data breach after third-party provider hacked - 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.