It's Probably Nothing
by Sierra Echo Charlie

EDITION 26 / 12 NOVEMBER 2026

N-central's fix isn't just a server upgrade

An emergency RMM hotfix, an exploited Outlook leak, and Git's server-side surprise.

5 stories / Listen online - 3:53

01 / THE BRIEF

N-central has a hotfix. Mind the rest of the fleet.

The N-central response has moved from keeping servers offline pending remediation to an available emergency build. Huntress and Rapid7 report that N-able released 2026.4 HF2, build 2026.4.1.26, on 10 November, addressing seven CVEs. That's a material change, but not an all-clear: Rapid7 says further security updates are planned.

WORTH ASKING

Rapid7 recommends keeping on-premises servers offline until successfully upgraded. Hosted and on-premises customers also need to update Agents first, then Probes, following vendor compatibility guidance. The server upgrade isn't the finish line.

QUALIFICATIONS

Before the hotfix, N-able reported scanning associated with the public proof of concept, but no evidence of successful exploitation in customer environments, according to both responders.

SOURCES

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

02 / THE BRIEF

Outlook’s exploited authentication leak needs an opened file

Microsoft has patched CVE-2026-124194, and CISA has added it to its Known Exploited Vulnerabilities catalogue. SecurityWeek quotes Microsoft saying that opening a crafted message file can make Outlook contact an attacker-controlled network location without the usual external-content warning, disclosing the user’s NTLMv2 hash.

The Preview Pane is explicitly excluded. This isn’t interaction-free code execution, but confirmed exploitation makes the 6.5 score a poor reason to leave it down the queue. Affected products include Microsoft 365 Apps for Enterprise and Office LTSC 2021 and 2024.

QUALIFICATIONS

SecurityWeek reports that Microsoft hasn’t disclosed details of the observed attacks.

SOURCES

CVE-2026-124194 - Microsoft Outlook Spoofing Vulnerability - Primary source

CISA Known Exploited Vulnerabilities catalogue, version 2026.11.10 - Primary source

Exploited Outlook Zero-Day Among 1,094 Flaws Patched by Microsoft - Reporting / context

The November 2026 Security Update Review - Primary source

Microsoft Patches Exploited Outlook Hash-Disclosure Zero-Day and Over 1,090 Flaws - Reporting / context

03 / THE BRIEF

Barracuda’s new requirement is investigation, not just patching

CISA has added both flaws in Barracuda’s ESG root-access chain to KEV, requiring forensic triage and setting a 13 November deadline for covered federal agencies. Exploitation isn’t the new development: Barracuda had already reported a small number of affected organisations on 9 November.

The distinction worth keeping straight: the unauthenticated chain requires access to ESG’s administrative interface, not valid credentials. It combines a crafted-backup authorisation bypass with command injection through the timezone field. Other listed Barracuda products have the administrator-required command-injection flaw, not the same unauthenticated chain.

SOURCES

CISA Known Exploited Vulnerabilities catalogue, version 2026.11.10 - Primary source

Pre-Authentication Authorization Bypass and Command Injection Vulnerabilities in Certain Barracuda Products - Primary source

MNDT-2026-0042 - Primary source

MNDT-2026-0041 - Primary source

Barracuda Flaws Reportedly Chain Into Unauthenticated Root Command Execution - Reporting / context

04 / THE BRIEF

Git’s fixes reach beyond the developer laptop

Git’s six security fixes include recursive-clone code execution through a long-path validation and truncation mismatch. Separately, CVE-2026-105437 lets a committed conflict-marker-size attribute turn small merge inputs into oversized output and heap corruption. GitLab says that can, under certain conditions, execute arbitrary commands inside Gitaly.

On forges that read repository-tree attributes for mergeability checks, pushing branches and requesting merges can trigger the overflow without another person acting, according to the CNA record.

WORTH ASKING

GitLab.com and Dedicated are patched. Official packages include patched Git; self-compiled installations need Gitaly’s embedded Git and the Git referenced by git.bin_path rebuilt or appropriately patched.

SOURCES

Git security vulnerabilities announced - Primary source

GitLab Critical Patch Release: 19.5.4, 19.4.6, 19.3.8 - Primary source

CVE-2026-105437 - Heap-based Buffer Overflow in Git - Primary source

Git Patches Six Flaws, Including Code Execution During Recursive Clones - Reporting / context

05 / THE BRIEF

Catch-up: Chrome’s exploited XML flaw

An earlier development worth catching up on: Google’s 9 November Chrome release fixed CVE-2026-125350 and acknowledged an exploit in the wild. Google’s description specifies code execution inside the sandbox through a crafted HTML page-not an established sandbox escape or complete device takeover.

WORTH ASKING

Fixed Stable versions are 157.0.8103.50/.51 for Windows and Mac, and 157.0.8103.50 for Linux. Google says rollout takes days or weeks, so checking the installed version is worthwhile.

SOURCES

Stable Channel Update for Desktop - Primary source

CVE-2026-125350 - Primary source

CISA Known Exploited Vulnerabilities catalogue, version 2026.11.10 - Primary source

Chrome Update Patches Exploited XML Zero-Day, Eighth This Year - Reporting / context

Chrome Patches XML Use-After-Free Flaw Reportedly Exploited in the Wild - 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.