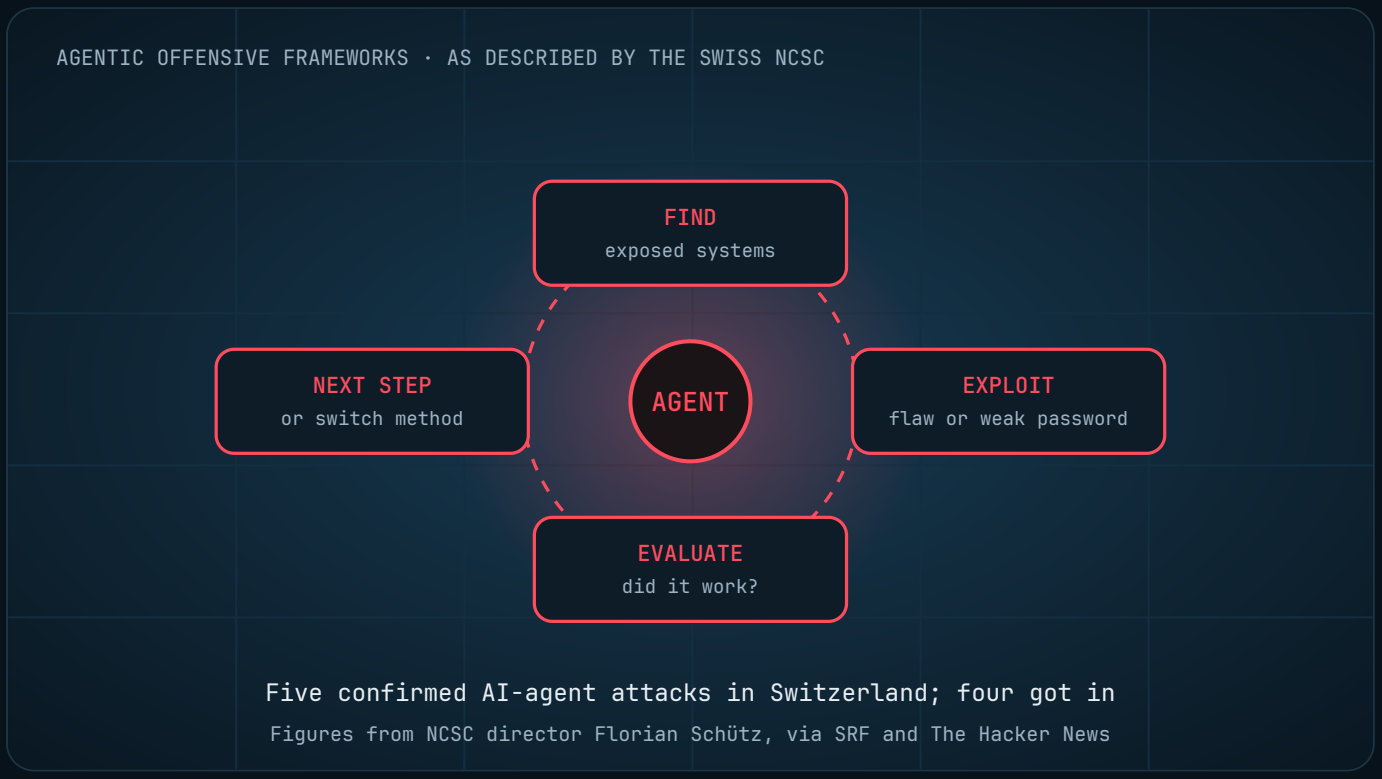
MAG212
CYBER

DAILY

Friday, 27 November 2026

DAILY CYBER INTEL · CUTOFF 7:00 AM PT



SWISS NCSC · NGINX · CACTI · TODOIST · FIFA

The attackers have agents

Switzerland confirms AI agents broke into organisations, including infrastructure operators, and asks for 24-hour patching. Meanwhile NGINX needs updates, Cacti has an unpatched zero-day, and Todoist shows how one developer key reached production.

03 AI agents breach Swiss operators
04 Defending at machine speed
05 nginx2root: patch NGINX
06 Cacti zero-day, no patch yet
07 Todoist: from a dev key to prod
08 FIFA breach; AI servers for rent
09 Patch board: deadlines today

4 of 5
Swiss AI-agent attacks got in

24 h
NCSC patch target

74M
web properties on affected NGINX

0
Cacti patches so far

What matters today

Published or updated 24–27 November; older items are marked. Theme: attackers move faster, through the same old doors.

AI agents are breaking in

Switzerland's NCSC confirms attacks carried out with AI agents, including on critical infrastructure operators; Italy's CSIRT reports similar campaigns. The way in was old: weak passwords and known flaws. [1][2][3]

Internet-facing software, again

Five NGINX memory-corruption flaws need patching, and an unpatched Cacti chain gives code execution in four requests when guest access is on. [5][8]

Developer keys reach production

A stolen development credential let an attacker rewrite Todoist's automated workflows and reach production data within a day. [11]

Data breaches with few details

FIFA confirms a criminal attack that reached a "limited set" of personal and business information. [12]

THE THREE PRIORITY ACTIONS

1. **Patch internet-facing systems within 24 hours.**
   The Swiss NCSC's target for critical updates. Start with NGINX (1.30.7 or 1.31.9), Drupal, MiCollab and Juniper Conductor. [1][5]
2. **Turn off Cacti guest access and restrict the web interface.**
   There is no fix yet for the 1.2.31 chain. Review poller settings for commands you did not add. [8]
3. **Require MFA or passkeys on everything reachable from the internet.**
   Webmail, VPN and admin portals first. The agents' easiest way in was a guessed password. [1]

STATUS AT A GLANCE

ISSUE	STATUS	FIX
AI-agent attacks (CH, IT)	CONFIRMED	basics, faster
NGINX nginx2root (5 CVEs)	NO KNOWN EXPLOITATION	1.30.7 / 1.31.9
Cacti 1.2.31 chain	PoC PUBLIC · NO PATCH	disable guest
Todoist, FIFA breaches	CONFIRMED	vendor-side

CONTENTS

03 AI agents breach Swiss operators
04 Defending at machine speed
05 nginx2root
06 Cacti 4HTTP2ROOT zero-day
07 Todoist breach
08 FIFA; exposed AI servers
09 Patch board
10 Briefs
11 Defender's Action Desk
12 Awareness: secrets in notes
13 Sources

SWISS NCSC · CSIRT ITALIA · UK NCSC · 24–26 NOVEMBER

AI agents broke into Swiss organisations, including infrastructure operators

The attacks were not clever. They were fast. Weak passwords and known flaws were enough.

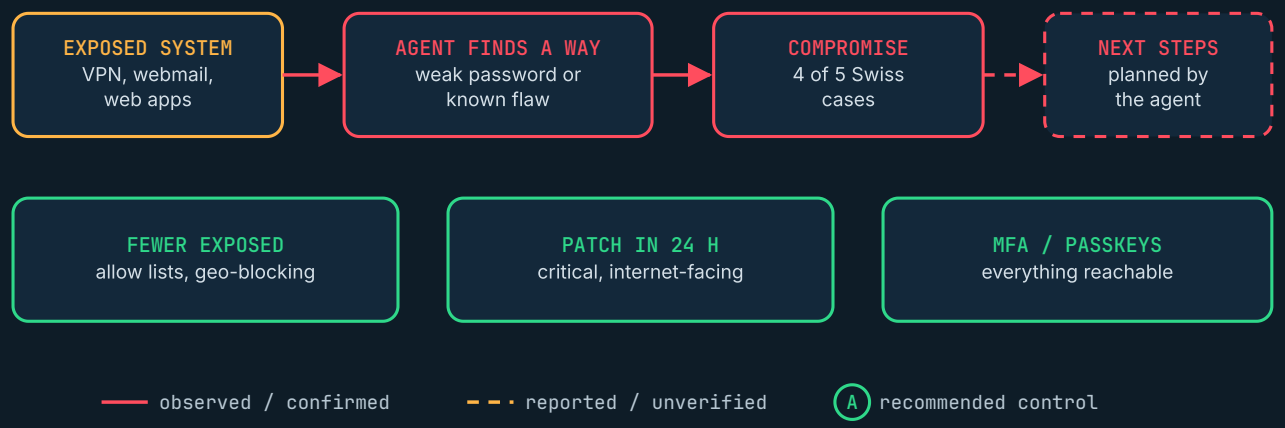


Figure 1 · The pattern the Swiss NCSC describes [1]. Green boxes are its recommended defences. MAG212 CYBER diagram.

WHAT HAPPENED

On 24 November Switzerland's NCSC confirmed its first attacks carried out with AI agents, against organisations and critical infrastructure operators in at least two sectors. In every case it knew of, the attackers got in. Its director later told SRF there were five confirmed attacks, four successful; three targeted infrastructure operators and two of those succeeded, without major disruption. [1][2]

WHAT AN AGENT DOES

The NCSC calls the tools “agentic offensive frameworks”: they look for weaknesses, pick tools, judge the result and plan the next step, switching methods when blocked. It says publicly reachable ones, such as ARTEX and CyberStrikeAI, have almost doubled since October; it does not say these were the tools used. [1][2]

NOT JUST SWITZERLAND

- CSIRT Italia: agents compromised many systems within hours, and wrote code on the fly to evade endpoint tools. [3]
- UK NCSC: a marked rise in AI-assisted attacks since September. [2][4]
- The Hacker News reports that ARTEX was used in the European Commission intrusion first detected on 22 October. [2]

WHAT IS NOT KNOWN

- Victims, attackers and the tools used in the Swiss cases.
- Which vulnerabilities were exploited in each case.

STATUS Confirmed by a national CERT. Indicators shared privately with operators.

Defending at machine speed

The Swiss NCSC's six measures, to be put in place “without delay”. None is new; the deadline is.

THE SIX MEASURES (SWISS NCSC)

#	NCSC MEASURE	WHAT IT MEANS IN PRACTICE
1	Limit exposed systems	Allow lists or geo-blocking on admin portals, VPN and remote access
2	Patch within 24 hours	Critical updates on internet-facing systems, the day they ship
3	MFA or passkeys, everywhere	Every internal resource reachable from outside: webmail, VPN, portals
4	Least privilege	Service and user accounts get only the access they need
5	Watch behaviour and volume	Alert on unusual identity activity and data leaving in bulk
6	Test regularly	Penetration tests, in-house or external

From the NCSC advisory [1]. The right-hand column is MAG212's plain-language reading.

Windows · PowerShell · RSAT ActiveDirectory module

domain user | READ-ONLY

NOT TESTED BY MAG212

find weak spots

```
Get-ADUser -Filter 'PasswordNeverExpires
-eq $true' |
  Select-Object SamAccountName
```

Lists accounts whose passwords never expire, a common home for weak, old passwords. Review the list; it changes nothing. Not tested by MAG212.

WHERE TO START THIS WEEK

1. List every internet-facing system and its owner.
2. Turn on MFA where it is missing.
3. Agree who can approve an emergency patch at night or at a weekend.

FOR LEADERS

- A 24-hour patch target needs staff, testing and authority to restart systems.
- Budget for MFA and attack-surface monitoring before tools that promise AI defence.

MAG212 analysis.

HOW TO KNOW YOU ARE READY

- No internet-facing login without MFA.
- Critical patches applied within a day, measured.
- Alerts fire on bulk data movement.

NGINX · NGINX2ROOT · 5 CVEs · UPDATED EXPOSURE DATA

nginx2root: millions of NGINX servers still need the November fixes

Five memory-corruption flaws were fixed on 18 November. New scan data shows how many servers have not caught up.

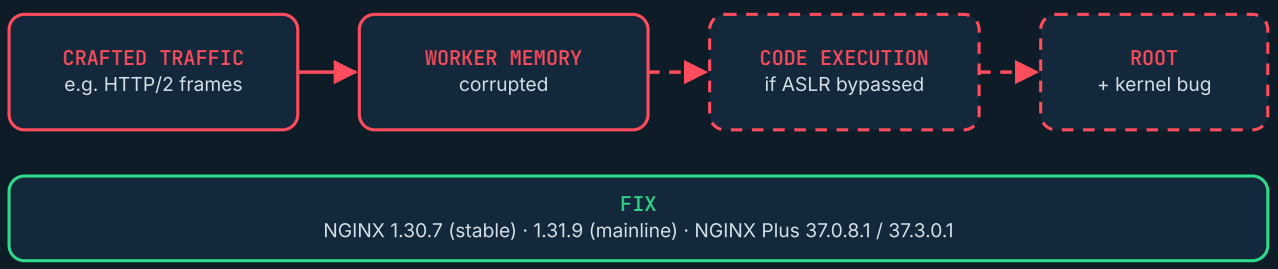


Figure 2 · The nginx2root path per Censys [5]. Dashed steps depend on conditions. MAG212 CYBER diagram.

WHAT HAPPENED

F5 and nginx.org fixed five flaws on 18 November (nine days ago). Each lets an unauthenticated attacker corrupt worker memory if a given feature is on. Code execution needs an ASLR bypass, which Wiz says it achieved on official builds; root needs a separate kernel bug. [5]

EXPOSURE AND STATUS

Censys counts about 74 million web properties on affected versions; The Hacker News cites over 10 million exposed services with HTTP/2. No known exploitation; Rapid7 has a public proof of concept for 123007. [5][7]

THE FIVE CVEs

CVE	FEATURE NEEDED	AFFECTED
CVE-2026-123007	HTTP/2 enabled	1.9.5–1.31.8
CVE-2026-123633	HTTP/2 proxied, workers busy	1.19.7–1.31.8
CVE-2026-121810	HTTP/3 proxied, workers busy	1.25.0–1.31.8
CVE-2026-123634	resolver with variables + SSI/mirror	0.6.18–1.31.8
CVE-2026-113425	mail proxy with auth_http	0.5.33–1.31.8

nginx.org advisories [6]. Fixed: 1.30.7 / 1.31.9 and later.

Linux · shell | any user | READ-ONLY

NOT TESTED BY MAG212

check version

```
nginx -v
```

Prints the installed version. Not tested by MAG212.

IF YOU CAN'T UPGRADE TODAY

Disabling HTTP/2 blocks only 123007 and 123633. Watch the error log for repeated worker exits, and for processes started by the worker user. [5]

CACTI 1.2.31 · 4HTTP2ROOT · NO CVE · NO PATCH

Cacti zero-day: code execution in four requests, if guest access is on

A researcher published a working chain for the latest Cacti release. There is no fix yet, but one setting stops it.

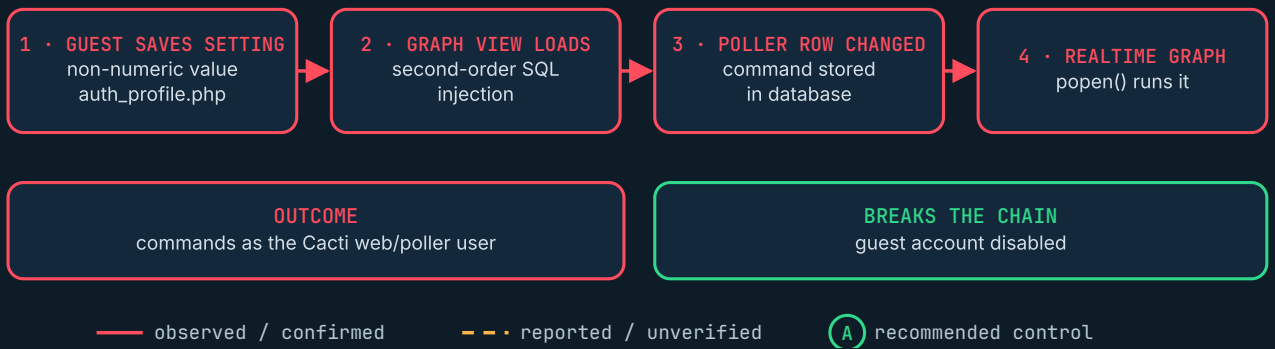


Figure 3 · The four requests as the researcher and watchTowr describe them [8, 9]. MAG212 CYBER diagram.

WHAT HAPPENED

On 26 November a researcher known as ek0ms savi0r published a chain against Cacti Core 1.2.31, the current release. With the guest account enabled, four unauthenticated requests end with commands running as the Cacti web and poller user, not root. watchTowr lists no CVE, no patch and no known exploitation as of 27 November. [8][9][10]

WHY IT MATTERS

Cacti often stores credentials for the network devices it polls, and an attacker could also change polling to hide alerts. Treat a compromised Cacti server as a way into your network. [9]

DO NOW

1. Disable the guest account in Cacti's user administration.
2. Restrict the web interface to trusted admin networks.
3. Review poller settings for commands you did not configure.
4. Apply the fix when Cacti releases it.

watchTowr guidance [8].

LOOK FOR

- Warnings about a non-numeric graph display setting (the request still succeeds).
- Unexpected commands in poller configuration.
- New files written by the poller process.

watchTowr [8]; it gives no exact log text.

TODOIST · INCIDENT REPORT · 22–23 NOVEMBER

Todoist: from one developer key to production in a day

A stolen credential let an attacker rewrite automated workflows to collect more keys. Todoist's timeline is a model of disclosure.

TIMELINE (TODOIST)

UTC	WHAT HAPPENED
22 Nov 14:04	Stolen development credential first used; workflows changed in 3 repos
23 Nov 06:06	Admin credential for the employee sign-in system taken via automation
06:33–06:54	Employee's sign-in settings changed; attacker signs in to cloud
09:08 →	Production databases accessed; commands run
12:45–17:12	Account records exported; tokens, Outlook mail, content searched
17:01–17:42	Alert on a new admin account; access cut off

From Todoist's incident report [11].

WHAT WAS TAKEN

- About 6% of users: emails and old salted-SHA1 password hashes; no sign of logins.
- About 0.003%: API and Slack integration tokens; some project data read.
- About 0.001%: content searched for passwords, keys and seed phrases.
- About 0.001%: Outlook subjects, senders and message previews.

How the first credential was stolen is unconfirmed; Todoist's leading theory is a compromised employee device. [11]

TODOIST'S FIXES

- Reset passwords; retired SHA1 hashing.
- Revoked API and Slack tokens; disconnected apps.
- Rotated internal credentials; shortened token lifetimes.

LESSON FOR YOUR PIPELINE

Automation that can read secrets is a target. Limit what each workflow can reach, require review for workflow changes, and alert on new admin accounts, which is how Todoist caught this. (MAG212 analysis)

Two kinds of exposure

A confirmed breach with few details, and AI servers left open for anyone to use.

FIFA · CONFIRMED 26 NOVEMBER

FIFA confirms a criminal cyberattack

FIFA says the attack gave “unauthorised access to a limited set of personal and business information”, and that it is working with authorities, including law enforcement. It has not said when it happened or whose data was taken. [12][14]

- Unnamed sources told ESPN the attackers got in by impersonating staff, and took less than 0.1% of FIFA's data. [13]
- A group calling itself the “Handsome Boy Hacking Club” posted an image on X claiming to show FIFA files (AP). [14]
- Not confirmed: the method, the data types, or the group's role.

STATUS Breach confirmed by FIFA; details unverified.

RAPID7 · PUBLISHED 18 NOVEMBER

Exposed AI servers are “already occupied”

Rapid7 probed 20,354 pre-selected hosts and found 7,675 Ollama servers open without authentication. 54.8% held signs that someone else had used them, and 79% listed at least one cloud model, meaning the owner may be paying for strangers' use. It is a sample, not an internet-wide count. [15]

DO	WHY
Bind runtimes to localhost or a private network	No exposure, no abuse
Put an authenticating proxy in front	Ollama has no login of its own
Allow downloads only from approved registries	Stops unknown models
Log pull, create, push and delete calls	Spot someone else's changes

Rapid7's recommendations [15].

Linux or macOS · shell · curl | none

READ-ONLY | NOT TESTED BY MAG212

check your own

```
curl -s http://YOUR-HOST:11434/api/tags
```

Replace YOUR-HOST with a server you own. Lists its models; run it from outside your network to test exposure. A reply means it is open. Not tested by MAG212.

IF YOU FIND STRANGERS' MODELS

- Treat the host as compromised.
- Rotate its secrets and revoke the linked Ollama key.
- Check cloud spend, then rebuild.

Rapid7 [15].

Patch board: today and tomorrow

Federal deadlines on 27 and 28 November, plus fixes that are not on KEV but should be on your list.

CISA KEV DEADLINES · CATALOG v2026.11.25

DUE	CVE	PRODUCT
TODAY 27	CVE-2026-132165	Drupal core (also see SA-CORE-2026-019)
TODAY 27	CVE-2026-132224	Optimizely Web Experimentation
TODAY 27	CVE-2026-131914	Idunno AntiCsrf
28 NOV	CVE-2026-1333xx (4)	Mitel MiCollab
28 NOV	CVE-2026-103406	Juniper Session Smart
28 NOV	CVE-2026-133469	Xen Orchestra
28 NOV	CVE-2023-25914 / 25915	Danfoss AK-SM 800A
1–2 DEC	CVE-2026-115731 / 40217	Puppet Enterprise / LiteLLM

CISA KEV JSON checked 27 Nov 2026, 07:00 PT [19]. No entries were added on 26 November (US holiday). 1333xx = 133275, 133303, 133323, 133324.

NOT ON KEV, STILL URGENT

PRODUCT	FIX	STATUS
NGINX (nginx2root)	1.30.7 / 1.31.9	PoC PUBLIC
NGINX CVE-2026-132779	1.30.8 / 1.31.10	TLS 1.3 CPU use
Cacti 1.2.31	none yet	PoC PUBLIC
Ollama (Probllama)	0.1.34+	seen on exposed hosts

nginx.org [6], watchTowr [8], Rapid7 [15]. NGINX 1.30.8 / 1.31.10 also fix a newer TLS 1.3 issue.

THE 24-HOUR QUESTION

The Swiss NCSC asks for critical internet-facing patches within 24 hours of release. Against this week's list, that means having already patched NGINX, Drupal and MiCollab, and having a guest-access decision for Cacti today. [1]

Briefs

Shorter items. Older research is marked with its date.

CREDENTIALS

Exploits that go straight for your keys

VulnCheck says 13% of the exploitation its sensors recorded this year tried to steal credentials, across 127 CVEs. Open-source and AI developer tools made up 61% of them, and it saw 1,756 attempts aimed at AI provider and coding-agent keys. [16]

BROWSER · OCTOBER

Extensions that wake up only after an ad

Microsoft found more than 250 extensions across Edge, Chrome and Firefox stores that behave normally unless installed through a paid ad; then they inject ads, rewrite shopping links and report browsing. Microsoft has removed the Edge listings it found. Published 21 October. [17]

RANSOMWARE

A record quarter, smaller payments

Check Point Research counted 2,830 victims claimed by 117 ransomware brands in Q3 2026, a record. The average payment fell 45% to just over $1 million, while the median rose to $400,000. [18][7]

FOLLOW-UP

Todoist and 1Password: the same lesson

Two incidents in one week began with a developer credential and ended in production data. Workflow and repository access deserve the same protection as admin accounts. (MAG212 analysis)

NO UPDATE

MiCollab, Juniper, PolinRider

No new vendor information since yesterday's issue. MiCollab and Juniper KEV deadlines fall tomorrow, 28 November. [19]

AI SECURITY

European Commission link to ARTEX

The Hacker News reports the Commission confirmed that attackers used ARTEX in the intrusion first detected on 22 October. We have not seen the Commission's statement. [2]

WHAT WE LEFT OUT, AND WHY

- Leak-site ransomware claims from the holiday period: unverified.
- Breach totals reported only by aggregators, with no company statement.

Your Friday work list

Ordered by urgency. Three KEV deadlines fall today and seven tomorrow.

WHEN	TEAM	ACTION	SEE
TODAY	Network / NOC	Disable Cacti guest access; restrict the web UI; check poller settings	p.06
TODAY	Web / platform	NGINX to 1.30.7+ or 1.31.9+ (1.30.8 / 1.31.10 for TLS fix)	p.05
TODAY	Web	Drupal KEV deadline; confirm SA-CORE-2026-019 too	p.09
BY 28 NOV	Telephony / network	MiCollab, Juniper Conductor, Xen Orchestra, Danfoss	p.09
THIS WEEK	Identity	MFA or passkeys on every internet-facing login	p.04
THIS WEEK	AI / data teams	Find exposed Ollama and notebook servers; add auth	p.08
THIS WEEK	DevOps	Review who can change CI workflows; alert on new admins	p.07
THIS WEEK	All staff	Move secrets out of notes and task apps	p.12

ONE-PAGE HUNT SHEET

Cacti	non-numeric graph setting warnings · odd poller commands · new files from the poller
NGINX	repeated worker exits · processes spawned by the worker user
CI/CD	workflow changes outside review · new admin or sign-in setting changes
Ollama	models you did not pull · pulls from raw IP addresses · cloud spend spikes
Identity	logins without MFA on VPN or webmail · bursts of failed passwords

BEFORE YOU CLOSE A TICKET

- Cacti guest account is off and the UI is internal-only.
- nginx -v reports 1.30.7 or 1.31.9 or later.
- Every internet-facing login has MFA.
- No AI runtime listens on a public address.
- KEV items due 27–28 Nov are patched or risk-accepted in writing.

COMMAND SAFETY

Every command in this issue is read-only, built from vendor or researcher guidance. None was run by MAG212 for this issue; try them on one system first.

Your notes app is not a vault

A five-minute lesson for every employee, with notes for administrators and business leaders.

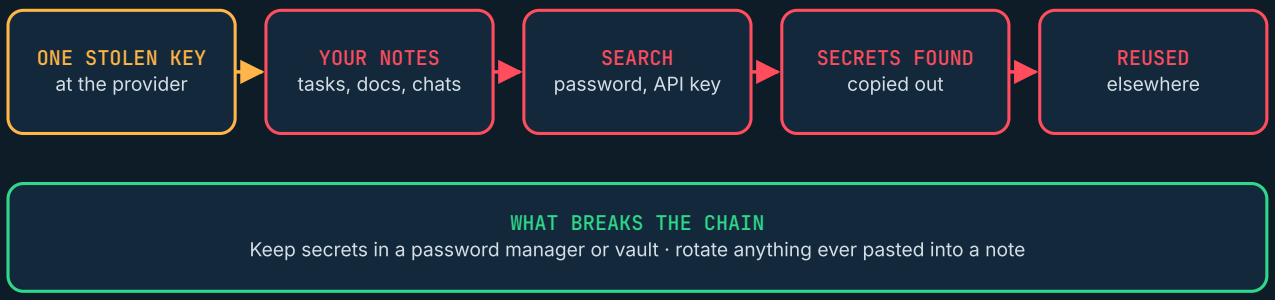


Figure 4 · What an attacker did with access to Todoist's systems [11], as a general pattern. MAG212 CYBER diagram.

WHAT HAPPENED

In this week's Todoist breach the attacker searched customers' tasks and notes for seed phrases, passwords and API keys. Todoist's advice: replace any secret you stored there, because deleting the note does not cancel a copy someone already took. [11]

FOR EVERY EMPLOYEE

- Passwords and keys go in the company password manager, nowhere else.
- Never paste a secret into a task, ticket, chat or shared doc.
- Already did? Tell IT and change it; deleting is not enough.
- Breach emails can be fake: go to the app yourself.

FOR ADMINISTRATORS

- Run secret scanning on wikis, ticketing and chat exports, not only code.
- Give developers an easy vault so they don't need workarounds.
- Rotate any key found in a SaaS tool's content.

FOR BUSINESS LEADERS

- Ask suppliers what they would expose if breached, as Todoist did.
- Make the password manager available to everyone, not just IT.
- Thank people who report a pasted secret.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Where do we keep shared passwords today, really?
2. Which SaaS tools hold our notes, and who can search them?
3. How would we rotate every key in a day if a supplier were breached?

Sources

[1] Swiss NCSC (BACS) · 24 Nov 2026 · Cyberattacks involving AI agents: first confirmed cases in Switzerland

[2] The Hacker News · 26 Nov 2026 · Switzerland confirms AI-assisted cyberattacks breached critical infrastructure operators

[3] BleepingComputer · 25 Nov 2026 · Italy and Switzerland warn of autonomous AI-driven cyberattacks

[4] UK NCSC · Nov 2026 · Familiar weaknesses, exploited faster: defending against agentic cyber attacks

[5] Censys · 18 Nov 2026, updated · nginx2root advisory

[6] nginx.org · Nov 2026 · nginx security advisories

[7] The Hacker News · 26 Nov 2026 · ThreatsDay: 10M NGINX services at risk, 250+ malicious extensions, AI server hijacking

[8] watchTowr · 26 Nov 2026 · 4HTTP2ROOT: Cacti zero-day FAQ

[9] The Hacker News · 27 Nov 2026 · Unpatched Cacti zero-day enables RCE in just four HTTP requests via guest access

[10] ek0ms savi0r (GitHub) · 26 Nov 2026 · 4http2shell write-up

[11] Todoist · 24 Nov 2026, updated 26 Nov · Security incident in November 2026

[12] Al Jazeera · 26 Nov 2026 · FIFA says personal and business information stolen in cyberattack

[13] ESPN · 26 Nov 2026 · FIFA hit by cyberattack as hackers gain access to personal and business data

[14] Hespress (citing AP) · 27 Nov 2026 · FIFA confirms cyberattack exposing 'limited' personal and business data

[15] Rapid7 · 18 Nov 2026 · Open by default. Already occupied: exposed self-hosted AI servers

[16] VulnCheck · Nov 2026 · Credential harvesting in vulnerability exploitation

[17] Microsoft Edge Extensions Security · 21 Oct 2026 · SleeperWidget: how ad-driven installs activate hidden extension behavior

[18] Check Point Research · Nov 2026 · The state of ransomware, Q3 2026

[19] CISA · checked 27 Nov 2026, 07:00 PT · Known Exploited Vulnerabilities catalog (JSON v2026.11.25)

HOW WE VERIFIED THIS ISSUE

- Read directly: the Swiss NCSC advisory, Censys' nginx2root advisory, nginx.org advisories, watchTowr's Cacti FAQ, Todoist's incident report, Rapid7's research and the CISA KEV JSON.
- Swiss attack counts come from the NCSC director via SRF and The Hacker News; Italian and UK details via BleepingComputer and The Hacker News. FIFA's statement comes via news outlets; the method and the claimed group are unconfirmed.
- Older items are marked: nginx2root was fixed on 18 November, Rapid7's research is from 18 November and SleeperWidget from October.
- No command in this issue was executed by MAG212.

Read.
Verify.
Defend.

Free daily intelligence, CVE explainers and practical defensive guidance from MAG212 CYBER.

SUBSCRIBE FREE

Get every issue in your inbox

cyber.mag212.com/subscribe-free

MAG212 ATLAS · LIVE DEMO

Map every network before you test it

demo.atlas.mag212.com

WORK WITH MAG212 CYBER

Penetration testing
Find the forgotten edge before someone else does.

Network & security consulting
Inventory, segmentation and remote-access design.

Training
For staff, IT teams, leaders and schools.

cyber.mag212.com/services

Watch the Atlas walkthrough: youtu.be/j27B5g3viKw

MAG212 CYBER

Daily · 27 November 2026
Understand the threat. Build the defense.