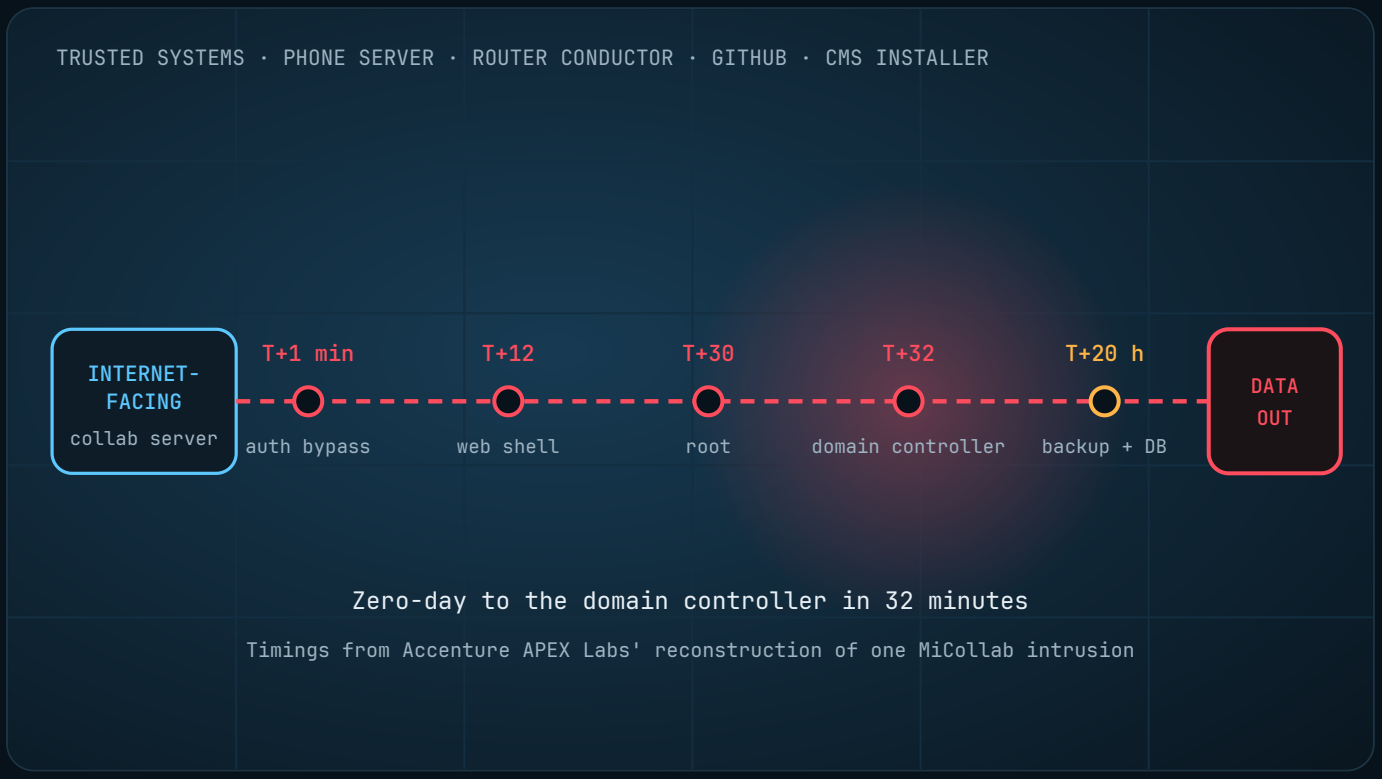
MAG212
CYBER

DAILY

Thursday, 26 November 2026

DAILY CYBER INTEL · CUTOFF 11:00 AM PT



MITEL · JUNIPER · 1PASSWORD · POLINRIDER · DRUPAL

32 minutes to the domain

Attackers used MiCollab zero-days to reach a domain controller in about half an hour. Juniper's router Conductor is under attack, 1Password lost data through one GitHub account, and Drupal's installer fix left a gap.

03 MiCollab zero-days, AI suspected
04 Hunting a MiCollab intrusion
05 Juniper Conductor exploited
06 1Password's GitHub breach
07 PolinRider poisons GitHub repos
08 Drupal's installer, round two
09 Patch board: 28 November

10.0
MiCollab command injection

9.8
Juniper Conductor, root

28 NOV
KEV due: Mitel, Juniper, Xen

375+
repos with PolinRider loader

What matters today

Published or updated 24–26 November. Theme: trusted systems used as the way in.

Collaboration servers as a way in

Accenture says attackers used five MiCollab flaws before Mitel's 16 November fix, reaching Active Directory and stealing data. All five are on KEV. [1] [2][4]

Router management, root access

Juniper now reports exploitation of a Session Smart Conductor command injection (CVSS 9.8) fixed on 28 October. CISA's deadline is 28 November. [4][5]

One developer account, wide reach

An employee's GitHub account gave an attacker 1Password source code and some customer account data; vaults were untouched. PolinRider plants loaders in developers' own repos. [8][10]

A fix that missed some sites

Drupal says sites left in an incomplete install state stayed open after last week's fix, and attackers are using that gap. [12]

THE THREE PRIORITY ACTIONS

1. **Patch MiCollab and hunt for the web shell.**
   Apply KB000129195 on 10.3.0.18 (or upgrade); until then, block external access to the AWV component. Image the server before rebuilding. [1][2]
2. **Upgrade Session Smart Conductor to 7.0.5, 7.1.7 or 7.2.3.**
   Keep Conductor management reachable only from admin networks, and check for unexpected provisioning activity. [5][6]
3. **Update Drupal to 10.6.23, 11.3.23 or 11.4.14 and run update.php.**
   Then check user 1's email and recent changes; secure the installer on every site. [12]

STATUS AT A GLANCE

ISSUE	STATUS	FIX
Mitel MiCollab (5 CVEs)	EXPLOITED · KEV	KB000129195
Juniper CVE-2026-103406	EXPLOITED · KEV	7.0.5 / 7.1.7 / 7.2.3
Drupal CVE-2026-136716	EXPLOITED · NOT KEV YET	10.6.23 / 11.3.23 / 11.4.14
1Password incident	CONTAINED (VENDOR)	no customer action

CONTENTS

03 Mitel MiCollab zero-days
04 Investigating MiCollab
05 Juniper Session Smart Conductor
06 1Password GitHub breach
07 PolinRider in GitHub repos
08 Drupal SA-CORE-2026-019
09 Patch board
10 Briefs
11 Defender's Action Desk
12 Awareness: the follow-up scam
13 Sources

MITEL MISA-2026-0012 · ACCENTURE APEX LABS · 5 CVEs ON KEV

MiCollab zero-days: from phone server to domain in 32 minutes

Accenture says attackers used five flaws before Mitel's patch, then went for Active Directory, backups and databases. It suspects AI tooling helped.

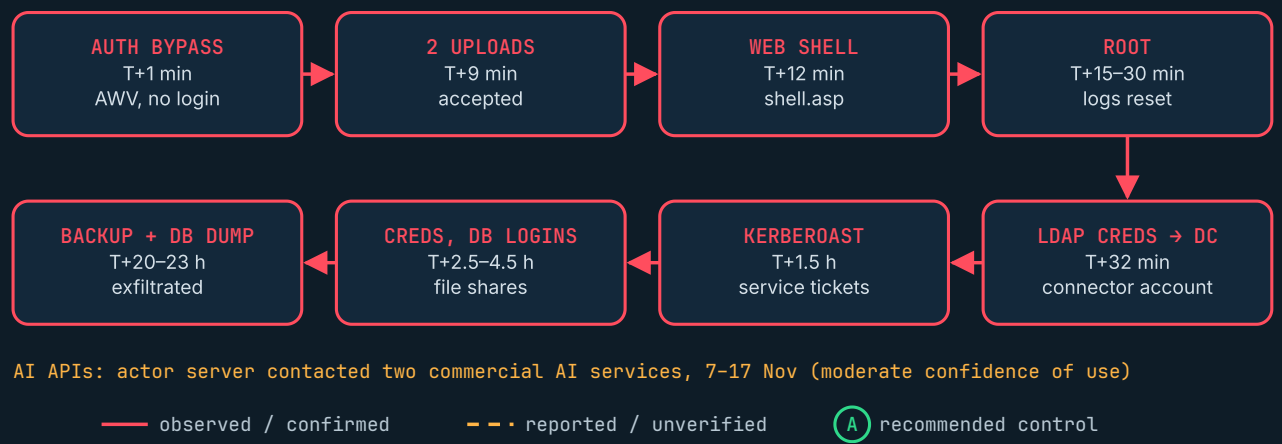


Figure 1 · One intrusion as Accenture APEX Labs timed it, from the first request [2]. Read left to right, then right to left. MAG212 CYBER diagram.

WHAT HAPPENED

Mitel's 16 November advisory fixed five unauthenticated flaws in MiCollab's Audio, Web and Video Conferencing (AWV) component, in 10.3.0.18 and earlier; it does not mention attacks. Accenture found a web shell at one victim before 23:00 UTC on 15 November, and a second server talking to the same attacker host since 9 November. CISA added all five on 25 November. [1][2][4]

THE AI QUESTION

The attacker's server contacted two unnamed commercial AI services; traffic restarted in the same second as the bypass request. Accenture has moderate confidence they were used, and names no group. It suspects data-theft extortion. [2]

THE FIVE CVEs

CVE	WHAT (AWV COMPONENT)	CVSS
CVE-2026-133323	Blind command injection	10.0
CVE-2026-133303	XML injection, pre-staged content	9.0
CVE-2026-133311	Sensitive information access	5.9
CVE-2026-133275	Arbitrary file upload	5.3
CVE-2026-133324	Authentication bypass	5.3

Mitel MISA-2026-0012 rev 2.0 [1]. Fix: KB000129195 on 10.3.0.18, or a later release. KEV due 28 Nov; CVE-2026-133311 due 9 Dec [4].

STATUS Exploited before the patch. In KEV. Patch available.

Hunting a MiCollab intrusion

Assume local logs were edited. Work from images, proxies and identity logs, and treat any hit as a possible Active Directory compromise.

WHAT TO LOOK FOR (ACCENTURE)

WHERE	LOOK FOR
Web root	New files under /pictures/ (shell.asp, shell.jsp); Java folders there
Web logs	POSTs to /awcuser/cgi-bin/ then new /pictures/ files; curl/8.14.1
/tmp	roast*.py, mkccache.py, testcreds*.py, relay*.py, *.tgz
Network	HTTP PUT to /bkup/; 204.76.203[.]204 and .216; trycloudflare, ipify
Identity	LDAP connector logging on to many DCs; bursts of RC4 Kerberos tickets

From Accenture APEX Labs [2]. Hunt 204.76.203[.]204 from 6 Nov and .216 from 12 Nov. A sudden drop in system log size is itself a signal.

MiCollab server (Linux) · shell | root | READ-ONLY | NOT TESTED BY MAG212

first look

```
ls -la /tmp
find / -path '*pictures*' \( -name
'*.asp' -o -name '*.jsp' \) 2>/dev/null
ss -tnp
```

Lists /tmp, finds script files in picture folders, and shows open connections. Paths vary by install. Run after imaging, not before. Not tested by MAG212.

CONTAIN, IN ORDER

1. Block external access to AWV, including any MiVoice Border Gateway path.
2. Image MiCollab and gateway servers.
3. Patch: KB000129195 on 10.3.0.18, or upgrade.
4. Patch older MiCollab flaws on lagging servers.

IF YOU FIND SIGNS

- Reset the LDAP connector account and Kerberoastable service accounts.
- Rotate admin, SIP trunk and file-share credentials the server could reach.
- Review domain controller logons and backup or database access.

HOW TO KNOW YOU ARE DONE

- Patched, and AWV not reachable from the internet.
- No unknown files, accounts or outbound connections.
- Connector and service accounts rotated; no new DC alerts.

JUNIPER SESSION SMART CONDUCTOR · CVE-2026-103406 · CVSS 9.8

Juniper's router Conductor is under attack

A command injection fixed a month ago is now exploited. The Conductor manages Session Smart Routers, so its compromise reaches the whole fleet.

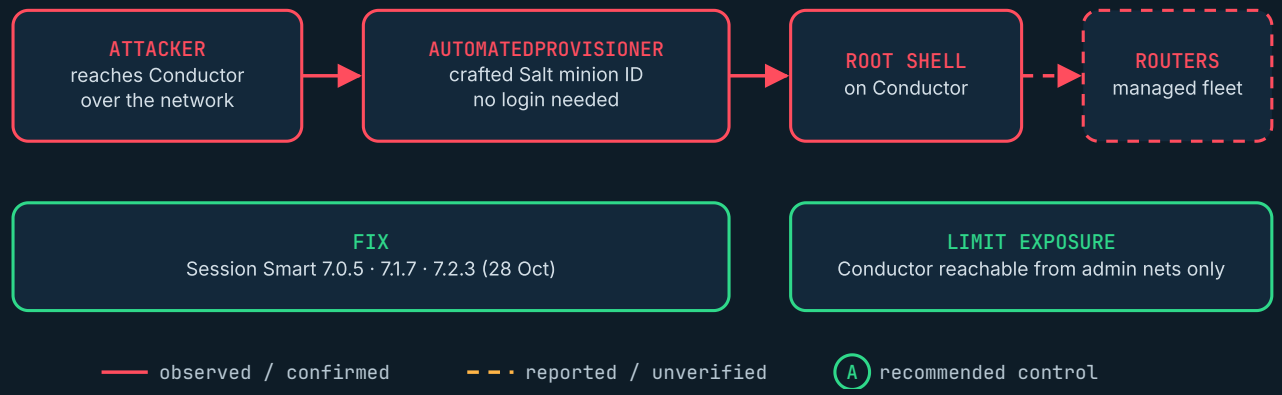


Figure 2 · The attack path in Juniper's description, via SecurityWeek and CISA [4, 5]. What an attacker did after getting root has not been published. MAG212 CYBER diagram.

WHAT HAPPENED

On 28 October Juniper fixed CVE-2026-103406 and 17 other Session Smart flaws. On 24 November it updated the bulletin: "At least one instance of malicious exploitation" was reported to its incident team. CISA added the flaw on 25 November, due 28 November, and its entry asks agencies to follow its new forensics-triage requirements. [4][5]

HOW IT WORKS

The AutomatedProvisioner service mishandles the Salt minion ID, the name a managed router uses to register with the Conductor. A crafted ID runs operating-system commands as root, with no login. [4][5]

WHAT IS NOT KNOWN

Who is exploiting it, how widely, and what they did next. No indicators have been published. [5][6]

AFFECTED AND FIXED

BRANCH	AFFECTED	FIXED
7.2	7.2.0-7.2.2	7.2.3
7.1	7.1.0-7.1.6	7.1.7
7.0	before 7.0.5	7.0.5

Applies to Conductor and Router [5, 6]. We could not load Juniper's bulletin directly [7].

INVESTIGATE

- Preserve logs and an image before upgrading.
- Review provisioning and registration activity for odd minion IDs.
- Look for new accounts, processes and config changes pushed to routers.
- Check credentials stored on the Conductor.

MAG212 guidance; no vendor indicators exist yet.

STATUS Exploited. In KEV, due 28 Nov. Fix available.

1PASSWORD · INCIDENT UPDATE · 25 NOVEMBER

One GitHub account opened 1Password's backend

An attacker used an employee's account to copy source code and push code that pulled customer account data. Vaults were not reached.

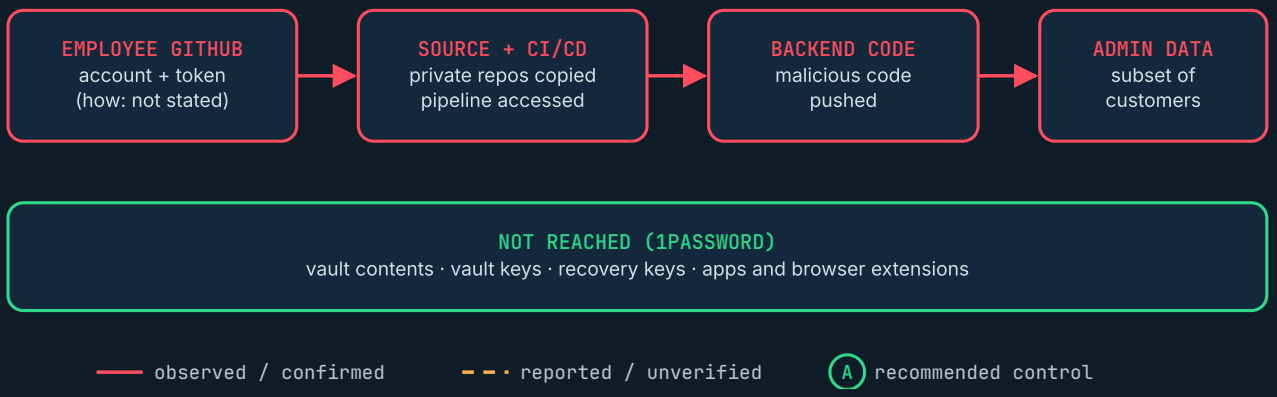


Figure 3 · The incident as 1Password describes it [8]. MAG212 CYBER diagram.

WHAT HAPPENED

1Password began investigating on 19 November and disclosed on 25 November. With an employee's corporate GitHub account and a stolen token, the attacker copied private source code, reached the CI/CD system, which holds infrastructure secrets, and pushed code to backend services that downloaded customer administrative data. 1Password has not said how the account was compromised, or how many customers are affected. [8]

WHAT WAS TAKEN

- Names, email addresses, account and user IDs, sign-up and last sign-in times.
- Public keys and Secure Remote Password (SRP) parameters.
- Tokens in some emailed invitation, provisioning and recovery links.

WHAT 1PASSWORD DID

- Disabled the account, revoked the token, rotated internal credentials.
- Restored clean versions of the affected service.
- Lengthened invite and recovery codes from 6 digits to 10 characters.
- Tightened GitHub, CI/CD and endpoint controls; brought in outside experts.

WHAT CUSTOMERS SHOULD DO

- No action is required, says 1Password.
- Expect phishing about invitations or recovery.
- 1Password never asks for your password or Secret Key.

See this week's awareness lesson (p. 12).

LESSON FOR EVERY SOFTWARE COMPANY

A developer account that can push to production is a production credential. Protect it with phishing-resistant MFA, short-lived tokens, branch protection and required reviews on deployable code. (MAG212 analysis)

SAFEDEP · APIIRO · POLINRIDER · GITHUB

PolinRider hides a loader in developers' own repositories

Thousands of GitHub projects now carry code that pulls its next stage from the Ethereum blockchain. The source is a developer's own machine.

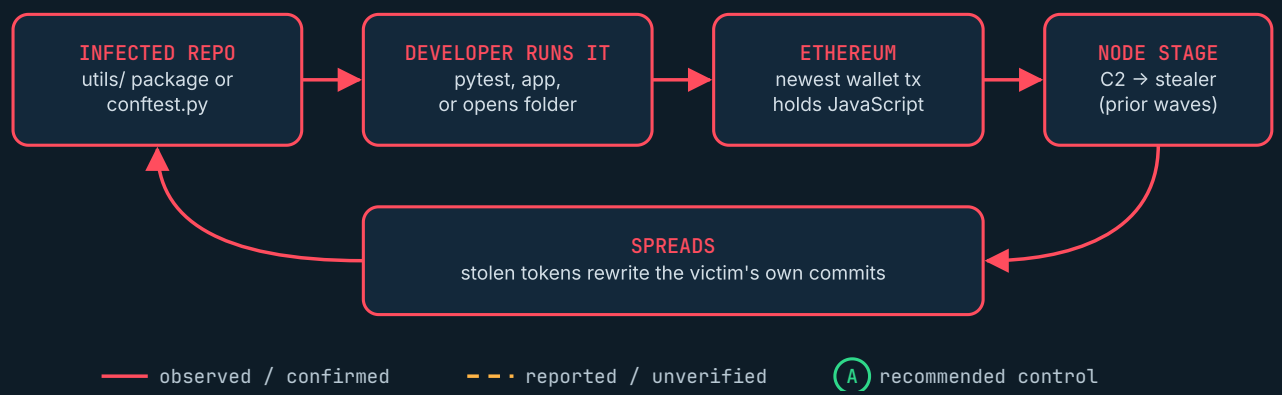


Figure 4 · How the Python loader runs and spreads, per SafeDep and Apiiro via The Hacker News [10, 11]. MAG212 CYBER diagram.

WHAT HAPPENED

SafeDep found a Python loader in 375 public repositories across 260 accounts; Apiiro estimates at least 7,609 repositories across 2,330 accounts, including 2,040 pushed between 27 October and 6 November. Researchers link PolinRider to North Korean actors and to the Contagious Interview fake-recruiter campaign; SafeDep itself names no group. [10][11]

HOW IT WORKS

The loader reads the newest transaction from a wallet, decodes JavaScript from it and runs it with Node, deleting the file and hiding errors. Apiiro says the worm rewrites a developer's commits with stolen access, keeping author and date. [10][11]

CHECK YOUR REPOS

- A `utils` (or lib, helpers, common) folder with session.py, transport.py, clients.py, http_session.py, net.py.
- Five new imports of those modules in main.py, app.py, asgi.py or cli.py.
- A `conftest.py` using `eth_getTransactionByHash`.
- Search all branches and history, not just HEAD.

SafeDep [10]. Your project may have its own utils package: check by hand.

IF YOU RAN IT

- Treat the machine as compromised.
- Rotate secrets, browser passwords and session cookies.
- Replace GitHub tokens and SSH keys; clean pushing machines.

DRUPAL CORE · SA-CORE-2026-019 · CVE-2026-136716 · 21/25

Drupal’s installer, round two: the fix missed some sites

Last week's patch did not cover sites in an odd install state. Attackers are using the gap, and a patched site may already have been taken over.

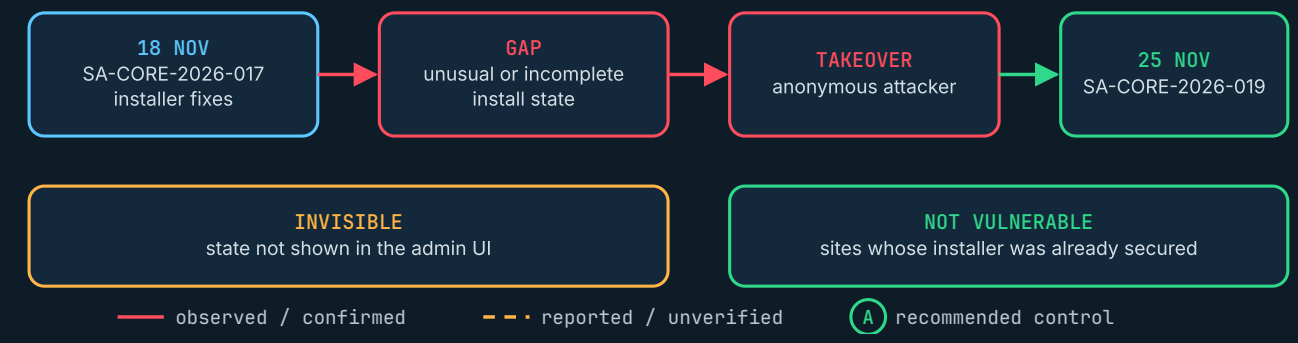


Figure 5 · What changed between the two advisories [12, 14]. MAG212 CYBER diagram.

WHAT CHANGED

On 25 November Drupal published SA-CORE-2026-019, an access bypass rated highly critical (21/25). Sites in “unusual or incomplete install states”, including production sites, stayed open to takeover after the 18 November fix. Drupal says: “This is being exploited in the wild.” [12]

WHY PATCHED SITES STILL NEED CHECKING

The vulnerable state is not visible in the interface, and a site that was already taken over may no longer look vulnerable. Any site that left its installer reachable after the first fix may have been compromised. If the installer was already secured, the site is not vulnerable. [12]

UPGRADE, THEN RUN UPDATE.PHP

BRANCH	UPDATE TO
11.4.x	11.4.14
11.3.x	11.3.23
10.6.x	10.6.23

The update hook must run to fix existing sites in this state [12].

CHECK FOR TAKEOVER

- Logs: unexpected changes to or by user 1.
- Is user 1's email address one you control?
- Consider resetting user 1's password.
- Secure the installer on every site.

Drupal's guidance [12]. Not yet in KEV at our check [4].

Patch board: a Thanksgiving pile-up

Federal deadlines land on 26, 27 and 28 November. Most organisations are not bound by them, but they are a good priority list.

CISA KEV DEADLINES · CATALOG v2026.11.25

DUE	CVE	PRODUCT	NOTE
TODAY 26	CVE-2026-133968	MONAI Label	0.8.6
TODAY 26	CVE-2026-134624	N-able Mail Assure	vendor-side
27 NOV	CVE-2026-132165	Drupal core	now -019 too
27 NOV	CVE-2026-132224 / 131914	Optimizely / Idunno	see 25 Nov
28 NOV	CVE-2026-103406	Juniper SSC / SSR	p. 5
28 NOV	CVE-2026-1333xx (4)	Mitel MiCollab	p. 3
28 NOV	CVE-2026-133469	Xen Orchestra	p. 10
28 NOV	CVE-2023-25914 / 25915	Danfoss AK-SM 800A	p. 10
1–2 DEC	CVE-2026-115731 / 40217	Puppet / LiteLLM	
9 DEC	CVE-2026-133311 · CVE-2025-41450	MiCollab · Danfoss	

CISA KEV JSON checked 26 Nov 2026, 11:00 PT [4]. Ten entries were added on 25 Nov [17]. CVE-2026-1333xx = 133275, 133303, 133323, 133324.

NEW ON KEV: WHAT EACH IS

- Mitel MiCollab: five AWV flaws, exploited as zero-days (p. 3).
- Juniper Session Smart: root command injection (p. 5).
- Xen Orchestra: login bypass with a crafted token (p. 10).
- Danfoss AK-SM 800A system managers: two 2023 flaws and one from 2025.

NOT ON KEV YET

- Drupal CVE-2026-136716 (SA-CORE-2026-019), exploited per Drupal.
- PolinRider has no CVE: it is malicious code, not a product flaw.

Absence from KEV does not mean no exploitation.

A NOTE ON CISA'S WORDING

This week's KEV entries point agencies to BOD 26-04, which ranks updates by risk, and to CISA's “Forensics Triage Requirements”: check whether a system was already compromised, not only whether it is patched. That is sound advice for everyone. [4]

Briefs

Shorter items, and follow-ups to this week's stories.

VIRTUALISATION

Xen Orchestra login bypass joins KEV

Vates warned on 10 November that a login bypass (VSA-2026-062) was being exploited: a crafted token gives admin rights, and Vates says that can lead to root on XCP-ng hosts. It is now CVE-2026-133469 on KEV, due 28 November. Vates' fix is in 6.10.1 and 6.9.2. [15][4]

OT · RETAIL

Danfoss AK-SM 800A flaws listed as exploited

CISA added three Danfoss AK-SM 800A flaws: path traversal and command injection from 2023 (due 28 November) and an information leak from 2025 (due 9 December). Old flaws on long-lived devices keep coming back. [16][4]

NETWORKING

Juniper's other 9.8 in the same bulletin

The October Session Smart bulletin also fixed CVE-2026-103409, which could give an unauthenticated attacker admin rights on Session Smart Router. It is not reported as exploited; the same upgrade fixes it. [6]

SUPPLY CHAIN

PolinRider tried pull requests too

A GitHub account, Eternity0207, opened more than 200 pull requests carrying the loader against projects including AsyncAPI Generator, CircuitVerse and Open Food Facts. GitHub has suspended it. Review contributors' changes to build files. [11]

UNIFIED COMMS

MiCollab: older servers too

Accenture's second victim ran a 10.0-series MiCollab, also open to older flaws (MISA-2026-0006). Its initial access is unknown. Lagging servers need both sets of fixes. [2]

IDENTITY

1Password customers: expect lures

Exposed names, emails and some link tokens make convincing phishing likely. 1Password says the tokens cannot grant access alone: SSO or an emailed code is also needed. [8][9]

THIS WEEK'S PATTERN: PATCHED IS NOT THE SAME AS CLEAN

MiCollab was attacked before its fix existed. Drupal says a patched site may already have been taken over. CISA's new KEV entries ask agencies for forensic triage, not just updates. After an exploited flaw, check for signs of past access as well as the version number. (MAG212 analysis) [2][12][4]

WHAT WE LEFT OUT, AND WHY

- Ransomware leak-site claims posted on 25–26 November: unverified, and some sites list fabricated victims.
- Breach totals reported only by aggregators, with no company statement we could find.

Your holiday-week work list

Ordered by urgency. Three KEV deadlines fall on 26, 27 and 28 November.

WHEN	TEAM	ACTION	SEE
TODAY	Telephony	Block external AWV access; patch MiCollab; image first if exposed	p.04
TODAY	Network	Upgrade Session Smart Conductor; limit management to admin nets	p.05
TODAY	Web	Drupal 10.6.23 / 11.3.23 / 11.4.14, run update.php, check user 1	p.08
BY 28 NOV	Virtualisation	Xen Orchestra 6.10.1 or 6.9.2	p.10
BY 28 NOV	Facilities / OT	Check Danfoss AK-SM 800A exposure and firmware	p.10
THIS WEEK	Dev / AppSec	Scan repos for PolinRider files; review build-file changes	p.07
THIS WEEK	Identity	Reset MiCollab LDAP connector if exposed; watch RC4 tickets	p.04
THIS WEEK	All staff	Warn about breach follow-up phishing	p.12

ONE-PAGE HUNT SHEET

MiCollab	/pictures/*/shell.asp · /tmp roast*.py, *.tgz · PUT /bkup/ · 204.76.203[.]204, .216
Juniper	odd Salt minion IDs · new accounts or processes on Conductor · unplanned router config pushes
Drupal	changes to or by user 1 · user 1 email changed · install.php requests
PolinRider	utils/ with session.py, net.py… · eth_getTransactionByHash · node -i without a terminal
Phishing	messages about 1Password invites or recovery asking for a password or Secret Key

BEFORE YOU CLOSE A TICKET

- MiCollab has KB000129195 (or later) and AWV is not internet-facing.
- Conductor and routers report 7.0.5, 7.1.7 or 7.2.3+.
- Drupal reports the new versions and update.php ran.
- Xen Orchestra reports 6.10.1 or 6.9.2+.
- Repos clean across all branches; tokens replaced where needed.

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.

After the breach, the follow-up scam

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

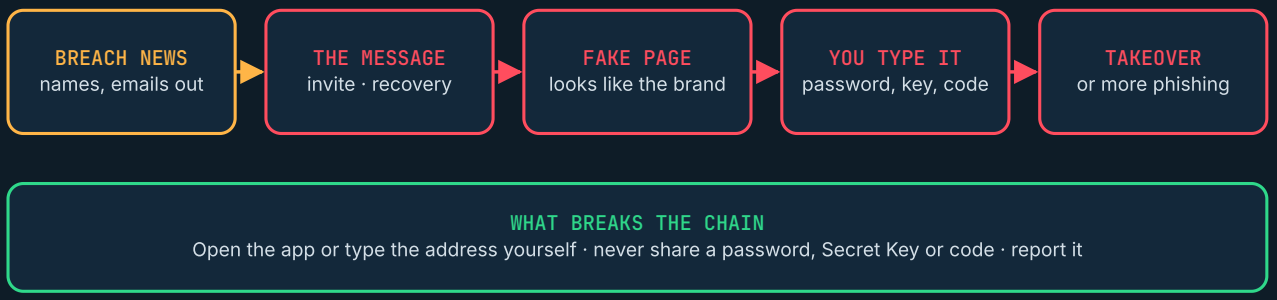


Figure 6 · How criminals reuse breach news. Generic model, not a specific campaign. MAG212 CYBER diagram.

WHAT IS HAPPENING

When a company says customer names and emails were exposed, scammers follow with messages about "your account", an invitation or a recovery. 1Password warned its customers this week to be wary of unexpected emails, texts or calls about invitations or recovery, and said it will never ask for an account password or Secret Key. [8]

FOR EVERY EMPLOYEE

- Don't use links in "security notice" emails. Open the app yourself.
- No real support team asks for your password, recovery key or code.
- Unexpected invitation or recovery email? Ask IT first.
- Report it, even if you clicked.

FOR ADMINISTRATORS

- If you use 1Password Business, tell staff what was exposed and what 1Password will never ask.
- Review pending invitations and recovery requests; cancel any you did not start.
- Tag external mail that mentions your password manager by name.

FOR BUSINESS LEADERS

- Send a short note to staff the day a supplier breach is in the news.
- Make reporting easy: one button or one address.
- Thank people who report; never punish them.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Which of our suppliers would we warn staff about if they were breached?
2. How would someone check whether an account email is real?
3. Who sends the warning, and how fast?

Sources

[1] Mitel · 16 Nov 2026, updated 24 Nov · MISA-2026-0012: MiCollab multiple vulnerabilities (rev 2.0)

[2] Accenture APEX Labs · Nov 2026 · MiCollab exploitation: zero-days used before Mitel's advisory

[3] SecurityWeek · 26 Nov 2026 · Mitel MiCollab zero-days exploited in suspected AI-assisted attacks

[4] CISA · checked 26 Nov 2026, 11:00 PT · Known Exploited Vulnerabilities catalog (JSON v2026.11.25)

[5] SecurityWeek · 26 Nov 2026 · Critical Juniper Session Smart Conductor flaw exploited in attacks

[6] eSecurity Planet · 26 Nov 2026 · Juniper Session Smart Conductor RCE exploited: CISA sets Nov. 28 deadline

[7] Juniper Networks · 28 Oct 2026, updated 24 Nov · 2026-10 On-Demand Security Bulletin: Session Smart Router and Conductor (could not be loaded)

[8] 1Password · 25 Nov 2026 · Update on November 2026 security incident

[9] The Hacker News · 26 Nov 2026 · 1Password hacked, customer data and source code stolen in GitHub account breach

[10] SafeDep · Nov 2026 · PolinRider Python loader reads payloads from Ethereum calldata

[11] The Hacker News · 26 Nov 2026 · North Korea-linked PolinRider poisons over 7,600 GitHub repositories

[12] Drupal Security Team · 25 Nov 2026 · SA-CORE-2026-019: Drupal core access bypass (highly critical)

[13] SecurityWeek · 26 Nov 2026 · Drupal installer patch left a gap attackers are already exploiting

[14] Drupal Security Team · 18 Nov 2026 · SA-CORE-2026-017: Drupal core, highly critical, remote code execution

[15] The Hacker News · Nov 2026 · Hackers exploit critical Xen Orchestra flaw (VSA-2026-062)

[16] Danfoss · 2023 · DSA-2023-08-01: AK-SM 800A security advisory

[17] CISA · 25 Nov 2026 · CISA adds 10 known exploited vulnerabilities to catalog

HOW WE VERIFIED THIS ISSUE

- Read directly: Mitel MISA-2026-0012, Accenture APEX Labs' report, 1Password's incident update, SafeDep's PolinRider analysis, Drupal SA-CORE-2026-019 and the CISA KEV JSON.
- Juniper's bulletin would not load; versions and dates come from SecurityWeek, eSecurity Planet and CISA. Apiiro's report would not load; its figures come via The Hacker News.
- North Korea attribution for PolinRider and AI use in the MiCollab attack are researchers' assessments, labelled as such. Unverified leak-site claims were left out.
- 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 · 26 November 2026
Understand the threat. Build the defense.