# MAG212 CYBER

DAILY

DAILY CYBER INTELLIGENCE

**Tuesday 10 November 2026**

Research cutoff: 06:15 PT (14:15 UTC) · Stories from the 24 h before 06:00 PT, extended to 72 h where labelled

# Attackers walk in through trusted doors

An exploited OpenSSH login bypass, a VPN flaw that skips SAML MFA, a vendor's own AWS account turned on its customers, and signed malware from a real release pipeline.

- **OpenSSH "sshole"** exploited on Alpine/musl · KEV due 12 Nov
- **Plex2Shell** hits Plex on QNAP NAS boxes
- **bee-js & Swarm Desktop** shipped signed malware
- **SonicWall SSL-VPN** SAML/MFA bypass · no workaround
- **Qubole's AWS account** used against its customers
- **France names IRGC-linked group** in fridge sabotage



By **El Mostafa Ouchen** · cyber.mag212.com

Free subscription: cyber.mag212.com/subscribe-free

*Cover art: conceptual illustration, MAG212 CYBER original. Not a real system.*

# Executive briefing

MAG212 ANALYSIS Today's thread is **trust that was granted once and never re-examined**. An OpenSSH bug lets attackers log in to Alpine and other musl-based Linux systems with an oversized password, and CISA gave federal agencies until **12 November** to fix it. A SonicWall SSL-VPN flaw skips SAML-enforced MFA. A data platform's own AWS account was used to assume roles its customers had created for it. A real release pipeline signed and published malware. Most fixes are configuration discipline, not new tools.

## The three actions that matter most today

**1** **Turn off password SSH on Alpine/musl hosts and containers, then patch and hunt**

Set `PasswordAuthentication no`, upgrade to your branch's fixed `openssh` package, restart sshd, then search logs for `Accepted password for` on passwordless accounts. ↗ Alpine ↗ CISA KEV

**2** **Upgrade every SonicWall firewall; close exposed NAS media ports**

SonicOS **7.3.4-7013** or **8.2.3-8015**, SAML SSL-VPN first (no workaround). On NAS boxes, stop forwarding Plex port 32400, update Plex and rotate passwords. ↗ SecurityWeek ↗ SecurityWeek

**3** **Audit vendor access into your cloud accounts**

List every IAM role that trusts a vendor account, starting with Qubole's `805246085872`. Delete unused ones, add source-IP or VPC-endpoint conditions, review CloudTrail from 1 October. ↗ The Hacker News

## Story board

| # | Story | Date label | Exploited? | Who should care |
|---|---|---|---|---|
| 1 | OpenSSH "sshole" auth bypass, CVE-2026-123158 | KEV 9 Nov, due 12 Nov | YES | Linux/container ops, network engineers, MSPs |
| 2 | SonicWall SSL-VPN SAML/MFA bypass, CVE-2026-19868 | 6 Nov · background, updated in window | YES | MSPs, schools, SMB firewall fleets |
| 3 | Plex2Shell on QNAP NAS | Reported 9 Nov | YES | Schools, SMBs, home offices |
| 4 | KEV batch: FreeSWITCH, GPUStack, IBM Faspex | KEV 9 Nov, due 12 Nov | YES | VoIP, AI/GPU platforms, file transfer |
| 5 | Qubole's AWS account used on customer roles | Reported 9 Nov | YES | Cloud teams, MSPs on AWS |
| 6 | France attributes fridge sabotage to IRGC-linked group | 9–10 Nov | YES | Retail, cold chain, healthcare, OT |
| 7 | Frontline Education breach rises to 3.08M | Updated 9 Nov | BREACH | School IT, healthcare, retail |
| 8 | bee-js / Swarm Desktop supply-chain compromise | 9 Nov | YES | Developers, DevOps, CI/CD owners |

### ⏳ Not out at the research cutoff, so not covered here

**Microsoft Patch Tuesday (10 Nov)** had not been published, so we give no zero-day or CVE counts; check the MSRC Update Guide. **Fortinet** said it would publish CVE IDs for critical FortiOS, FortiManager, FortiAnalyzer, FortiMail and FortiAuthenticator fixes by 10 November; publication had not been confirmed. ↗ Cybernews Details: Watch today.

# In this issue


**01** **OpenSSH "sshole": an oversized password opens the door** 4
Alpine/musl sshd without PAM · KEV due 12 Nov

**02** **SonicWall SSL-VPN flaw sidesteps SAML MFA** 6
SonicOS Gen7/Gen8 · no workaround

**03** **Plex2Shell hits Plex Media Server on QNAP NAS** 8
Four unauthenticated RCE flaws · port 32400

**04** **Three more on a three-day KEV clock** 9
FreeSWITCH · GPUStack · IBM Aspera Faspex

**05** **Qubole's own AWS account turned on its customers** 10
Cross-account IAM role abuse · published IOCs

**06** **France blames Iran's IRGC for heating supermarket fridges** 12
Refrigeration controllers become a nation-state OT issue

**07** **Frontline Education breach doubles to 3.08 million** 14
Plus Amplifon and Revolve count updates

**08** **Signed, provenanced and malicious: bee-js and Swarm Desktop** 15
Hijacked maintainer and release-bot accounts

◆ **Defender's Action Desk** 17
Prioritised checklist · KEV deadlines this week · watch today

◆ **Awareness lesson: "The breach letter is the bait"** 18
For employees and leaders · briefly noted

◆ **Source register** 20
Every source, with whether we could open it


## How to read this issue

**CONFIRMED** stated by a primary source: vendor, researcher or government.

**REPORTED** from a secondary outlet, or a claim that outlet attributes to someone.

**MAG212 ANALYSIS** our editorial judgement, not a source claim.

**UNKNOWN** not established by any source we read.

Links marked ↗ like this point to the source for the claim beside them. Diagrams are original MAG212 CYBER work built from those sources; none is a screenshot, photo or live data. Commands come from vendor documentation and were **not tested** by MAG212 CYBER.

### Evidence limits today

- cisa.gov and the NVD API were unreachable during research. KEV data comes from CISA's official GitHub mirror, catalog **v2026.11.09**. ↗ CISA KEV JSON
- **No NVD CVSS score was verified** for any CVE in this issue; scores shown are vendor or reported scores.
- We could not open the SonicWall PSIRT page, the FreeSWITCH GitHub advisory, Wiz's Qubole post, Apiiro's post or the IC3 refrigeration advisory PDF. Those details rest on the trade-press reports cited.

ACTIVELY EXPLOITED · LINUX & CONTAINERS

01

# OpenSSH "sshole": an oversized password opens the door

Exploited | KEV due 12 Nov | Fix 5 Nov · KEV 9 Nov | Evidence: strong

| CVE | AFFECTED | FIXED | CVSS |
|---|---|---|---|
| CVE-2026-123158 | sshd on musl libc, no PAM (Alpine default) | OpenSSH 10.6p2 · Alpine packages below | Not verified |
| **KEV** | **NOT AFFECTED** | | |
| Added 9 Nov · due 12 Nov · forensic triage | glibc distros, PAM setups, Dropbear (reported) | | |

## What happened

CONFIRMED OpenSSH 10.6p2, released on **5 November**, includes a "critical security workaround" for Linux systems that use musl libc with PAM disabled. The release notes say the root cause is outside sshd but can be avoided there, and do not cite a CVE. ↗ OpenSSH Alpine published its advisory the same day. ↗ Alpine On **9 November** CISA added **CVE-2026-123158** to the Known Exploited Vulnerabilities (KEV) catalog with a **12 November** due date and a forensic-triage flag. ↗ CISA KEV

REPORTED Previdian saw a first exploitation attempt less than nine hours after the CVE was published and confirmed root access on an Alpine honeypot. ↗ Help Net Security SecurityWeek reported on 9 November that botnets and cryptominers are exploiting it. ↗ SecurityWeek OpenSSH's Damien Miller told affected users to set `PasswordAuthentication=no` or disable SSH "IMMEDIATELY". ↗ Help Net Security

## Who is affected

CONFIRMED Per Alpine, a system is exploitable only when **all** of the conditions in the diagram hold. You are **not** affected with `openssh-server-pam` and `UsePAM yes`, with `PasswordAuthentication no`, on locked ( `!` ) accounts, with no `$`-style hashes on the host, or in containers that don't run sshd. Root is protected by the default `PermitRootLogin prohibit-password`, unless another account can escalate, for example through doas. Affected Alpine tiny-cloud images run from 3.18.11 to 3.24.3; fixed point releases are 3.21.10, 3.22.8, 3.23.8 and 3.24.4. ↗ Alpine

REPORTED The researcher names OpenWrt, Buildroot, Yocto and "a lot of the docker images" as other musl-based systems. Alpine AWS and Azure tiny-cloud images 3.18.11–3.24.3 ship a default `alpine` user with passwordless doas. Debian, Ubuntu, Fedora, Dropbear and OpenBSD are reported unaffected. ↗ Help Net Security

MAG212 ANALYSIS The main exposure is Alpine-based containers and VMs running sshd, plus embedded builds. Check each network vendor for OpenWrt-based routers and access points rather than assuming either way; many use Dropbear. We found no network-vendor advisory.

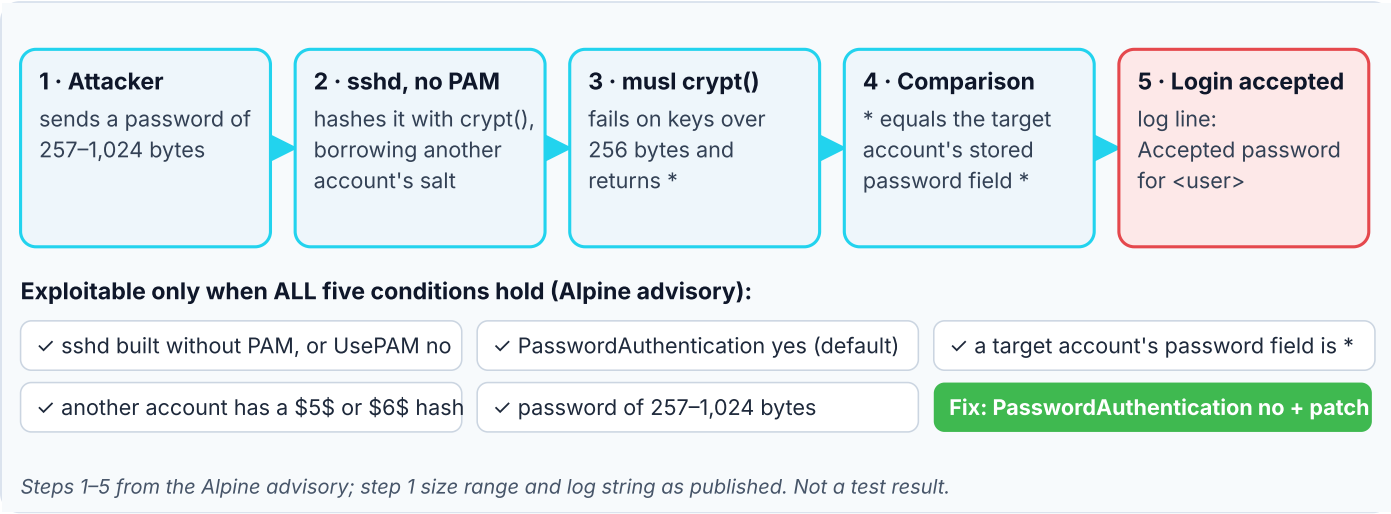



**Figure 1 · How the sshole bypass works.** The five-step chain and the five conditions that must all be true. Setting PasswordAuthentication no stops step 1 from reaching the vulnerable code path.
*MAG212 CYBER original diagram, based on the Alpine Linux advisory (5 Nov 2026).*

## How the attack works

CONFIRMED Without PAM, sshd hashes each password attempt with `crypt()`. If an account's stored field is too short to hold a salt, sshd borrows another account's salt. musl's `crypt()` fails on keys longer than 256 bytes and returns `*`, which matches a stored `*` password field, so the login succeeds. ↗ Alpine REPORTED On Previdian's honeypot the attacker ran `id`, `uname` and `hostname` after logging in. ↗ Help Net Security UNKNOWN CVSS score, worldwide exposure, and payloads beyond botnet and cryptominer activity.

## What to look for

- VENDOR GUIDANCE In `/var/log/messages`, `Accepted password for` on accounts that have no password, such as `alpine`, `root` and key-only users. Also review doas use, newly created users and `authorized_keys` changes. ↗ Alpine
- SINGLE HONEYPOT INDICATOR All eight attempts Previdian saw came from `89.116.89[.]18`. Treat it as one data point, not a blocklist. ↗ Help Net Security
- MAG212 ANALYSIS False positives: legitimate password logins on accounts that do have a password. The signal is a successful password login on an account whose password field is `*`.

## Investigate, contain and remediate (in order)

1. **Stop the bleeding.** If you can't patch now, disable password authentication (panel 2) or disable SSH on the system. ↗ Alpine
2. **Patch** to your branch's fixed package (table) or upstream OpenSSH 10.6p2.
3. **Restart sshd.** Alpine notes the upgrade does not restart a running sshd.
4. **Hunt** with the log and account checks above on every host that met the conditions.
5. **Decide on compromise.** "If a login cannot be ruled out, treat the machine as compromised." ↗ Alpine
   MAG212 ANALYSIS For containers and cloud images, rebuild from a patched image and rotate credentials the host held.

| Alpine branch | Fixed `openssh` package | Alpine branch | Fixed package |
|---|---|---|---|
| edge | `10.6_p2-r0` | 3.20 | `9.7_p1-r6` |
| 3.24 | `10.3_p1-r2` | 3.19 | `9.6_p1-r3` |
| 3.23 | `10.2_p1-r1` | 3.18 | `9.3_p2-r4` |
| 3.22 | `10.0_p1-r11` | 3.17 | `9.1_p1-r7` |
| 3.21 | `9.9_p2-r1` | 3.16 | `9.0_p1-r6` |

Source: Alpine advisory, 5 Nov 2026.

**Panel 1 · Patch** OS: Alpine Linux Shell: sh (ash) Privileges: root **CHANGE**

```
# Upgrade all packages, including openssh
apk upgrade -U -a
# Restart sshd; the upgrade does not do it for you
rc-service sshd restart
```

Interpretation: after the restart, the installed openssh should match the table. Commands not tested by MAG212 CYBER; syntax from the Alpine advisory.

**Panel 2 · Workaround** OS: Alpine Linux Shell: sh (ash) Privileges: root **CHANGE**

```
# Create /etc/ssh/sshd_config.d/00-no-passwords.conf containing the line:
PasswordAuthentication no
# Validate the config; restart only if validation passes
sshd -t && rc-service sshd restart
```

Make sure key-based access works before you rely on this, or you may lock yourself out. Not tested by MAG212 CYBER; syntax from the Alpine advisory.

**Panel 3 · Verify** OS: Alpine Linux Shell: sh (ash) Privileges: root **READ-ONLY**

```
# Show the effective setting sshd is using
sshd -T | grep -i passwordauthentication
```

Expected where the workaround is applied: `passwordauthentication no` (illustrative output). Not tested by MAG212 CYBER; syntax from the Alpine advisory.

## Verify recovery

Confirm the installed `openssh` package matches the table for your branch, that sshd was restarted after the upgrade, and that `sshd -T` reports password authentication off wherever you applied the workaround. Re-run the log check to be sure no new `Accepted password for` entries appear on passwordless accounts.

## Prevention and awareness

**MAG212 ANALYSIS** Make key-only SSH the baseline, and don't run sshd in containers that don't need it. Container base images inherit their OS's authentication quirks. **REPORTED** Previdian warns that proof-of-concept code on GitHub is unverified and could contain malware; don't run it to "test" production. ↗ Help Net Security

EXPLOITED · REMOTE ACCESS VPN

02

# SonicWall SSL-VPN flaw sidesteps SAML-enforced MFA

**Exploited (KEV)** **No workaround** **Advisory 6 Nov · background, updated in window** **Evidence: medium–strong**

| CVE | AFFECTED | FIXED | CVSS |
|---|---|---|---|
| CVE-2026-19868 (CWE-308) | Gen7 ≤ 7.3.3-7015 · Gen8 ≤ 8.2.2-8015 | 7.3.4-7013 · 8.2.3-8015 | 7.1 vendor (7.5 CISA-ADP, secondary) |
| **CONDITION** | **KEV** | | |
| SSL-VPN set to SAML authentication | Added 6 Nov · due 20 Nov | | |

## What happened

CONFIRMED CISA added **CVE-2026-19868**, a SonicOS SSL-VPN "use of single-factor authentication" flaw, to KEV on **6 November** with a **20 November** due date. ↗ CISA KEV REPORTED SonicWall advisory SNWLID-2026-0014 fixes seven SonicOS flaws. SonicWall says it "investigated a report of potential exploitation" of this one, without details, and scores it 7.1. ↗ BleepingComputer ↗ SecurityWeek CISA's flagging was covered on 9 November. ↗ The Hacker News

## Who is affected

REPORTED Gen7 TZ/NSa/NSsp/NSv on SonicOS 7.3.3-7015 or older, and Gen8 TZ/NSa/NSv on 8.2.2-8015 or older, but only where **SSL-VPN is configured for SAML authentication**. There is no workaround. ↗ SecurityWeek The same advisory fixes two management-interface flaws rated 8.8 (CVE-2026-107155, CVE-2026-107154), a pre-auth SSL-VPN heap overflow causing denial of service (CVE-2026-82308, 7.5), two TACACS+ issues (5.9 each) and weak password hashing on virtual appliances (5.2); their exploitation status is not stated. ↗ Oflight digest

MAG212 ANALYSIS MSPs and schools that put SSL-VPN behind Entra ID or Google SSO through SAML are directly exposed. Fleets without SAML still need the update because of the 8.8 management-interface flaws.

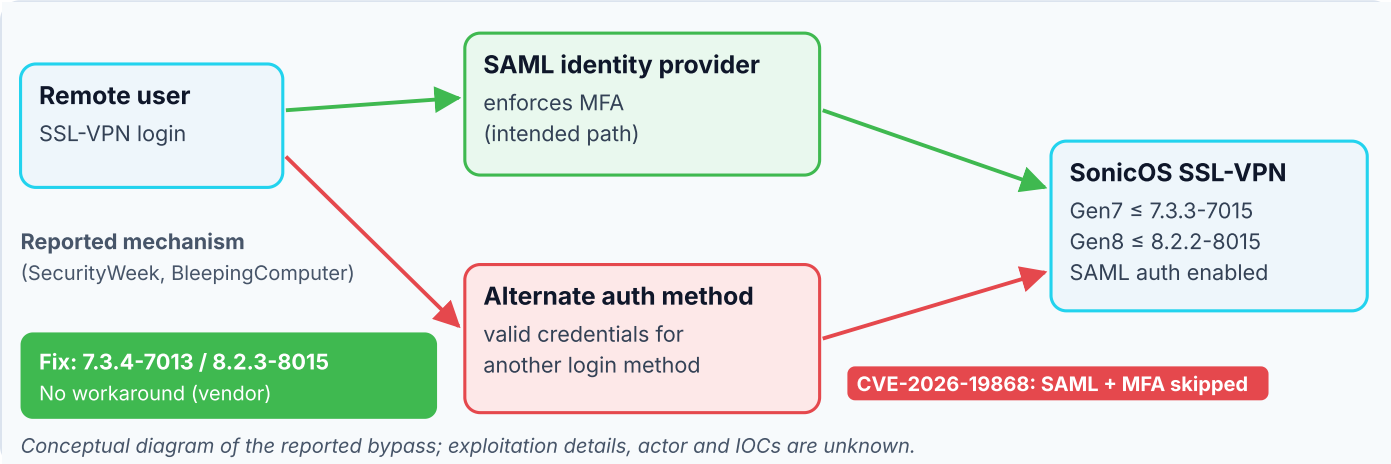



**Figure 2 · Intended SAML path versus the reported bypass.** Users should reach the SSL-VPN through the SAML identity provider that enforces MFA (green). With CVE-2026-19868, valid credentials for an alternate method reach the VPN without SAML or MFA (red). *Conceptual MAG212 CYBER original diagram, based on SecurityWeek and BleepingComputer reporting. Not an incident reconstruction.*

## How the attack works

REPORTED A user who holds valid credentials for an **alternate authentication method** can bypass SAML controls, including SAML-enforced MFA, on SSL-VPN logins. ↗ SecurityWeek UNKNOWN Who exploited it, how widely, where the alternate credentials came from, and any IOCs; none were published. No source links it to ransomware.

MAG212 ANALYSIS SSL-VPN is a common initial-access route, which raises the stakes.

## What to look for and how to investigate

If SAML SSL-VPN is enabled, review VPN logins that authenticated through an alternate method rather than SAML. ↗ SecurityWeek We could not open SonicWall's PSIRT page, so we don't reproduce its GUI path or detection guidance; read SNWLID-2026-0014 before acting. Interface labels vary by SonicOS version.

## Contain and remediate (in order)

1. Inventory every SonicWall on Gen7 ≤ 7.3.3-7015 or Gen8 ≤ 8.2.2-8015 and flag those with SAML SSL-VPN.
2. Upgrade to **7.3.4-7013** or **8.2.3-8015**; there is no workaround. ↗ SecurityWeek
3. Restrict the management interface, which has its own 8.8 flaws. ↗ SecurityWeek
4. MAG212 ANALYSIS Where alternate-method logins look suspicious, reset those credentials and review what the sessions reached.

## Verify recovery

Confirm each device's firmware is at or above the fixed build. Then confirm new SSL-VPN sessions on SAML portals show SAML/MFA completion, not alternate-method authentication. **Commands:** none were sourced from SonicWall documentation, so none are given.

## Prevention and awareness

MAG212 ANALYSIS MFA enforced at an identity provider protects only the login paths that go through it. Any parallel authentication method on the same portal is a bypass waiting to happen: inventory them and turn off the ones you don't need.

EXPLOITED · NAS & MEDIA SERVERS

# Plex2Shell hits Plex Media Server on QNAP NAS

03

Widespread exploitation | Reported 9 Nov · exploited since mid-Oct | Evidence: medium

| CVES | TYPE | FIXED | NOT AFFECTED |
|---|---|---|---|
| CVE-2026-96652, -96654, -96655, -96656 | Unauthenticated RCE chain | Plex Media Server 1.43.3.10861 or later | QTS and QuTS hero themselves |

## What happened and who is affected

REPORTED QNAP warned of widespread exploitation of **Plex2Shell**, a chain of four unauthenticated remote-code-execution flaws in Plex Media Server, since mid-October after proof-of-concept code was published. Some users report their Plex servers appear compromised. QNAP says QTS and QuTS hero are not affected and no data loss has been reported. ↗ SecurityWeek QNAP's notice is titled for an update to 1.43.3.10861 or later; SecurityWeek says 1.43.3 or later. We follow the more specific build. ↗ QNAP notice

UNKNOWN The actor, payloads, any ransomware link (none reported) and IOCs (none published).

MAG212 ANALYSIS Schools and SMBs running Plex on a NAS with port 32400 forwarded to the internet are exposed, and a NAS often holds the backups you'd need to recover from a wider incident.

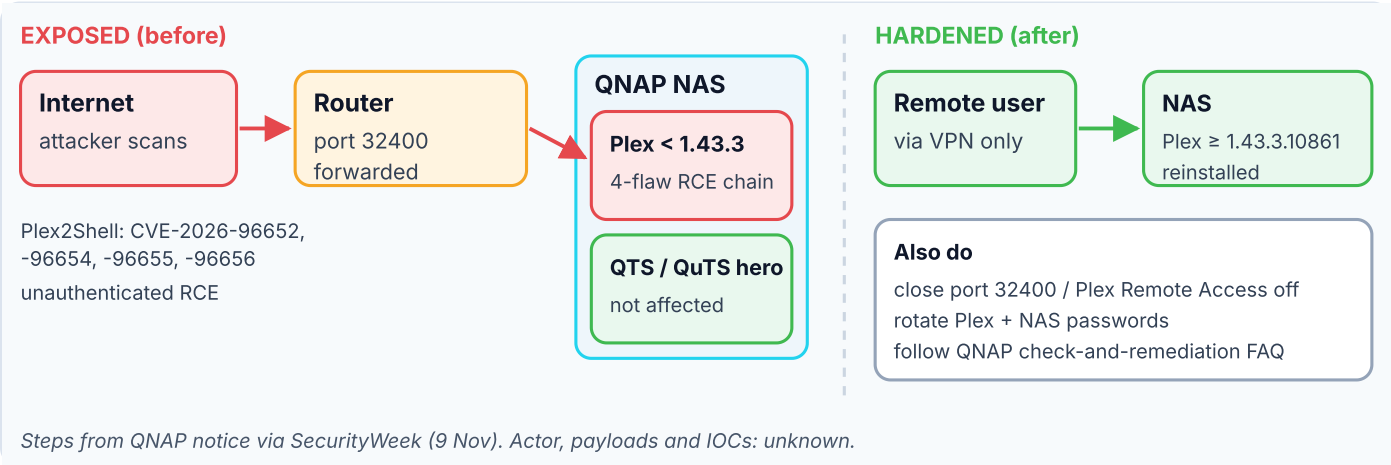



**Figure 3 · Exposed versus hardened Plex on a NAS.** Left: port 32400 forwarded straight to a vulnerable Plex Media Server. Right: remote access only through a VPN, Plex reinstalled and updated, port closed, passwords rotated.
*MAG212 CYBER original diagram, based on QNAP's notice as reported by SecurityWeek (9 Nov 2026).*

## How the attack works

Only the outline is published: four flaws chained for unauthenticated code execution in Plex Media Server, reachable where the server is exposed. The individual steps and payloads were not described in the sources we read, so we don't speculate.

## What to look for, investigate, contain and remediate (in order)

1. Treat internet-exposed devices as **potentially compromised**. ↗ SecurityWeek
2. Disable Plex Remote Access and **stop forwarding port 32400**; use a VPN if remote access is needed.
3. **Reinstall Plex** and update to 1.43.3.10861 or later.
4. **Rotate** Plex and NAS passwords.
5. Work through QNAP's check-and-remediation FAQ; MAG212 did not review its contents.

## Verify recovery and prevention

Confirm the Plex version, that port 32400 no longer answers from outside your network, and that passwords changed. MAG212 ANALYSIS Apps installed on a NAS widen its attack surface: a secure NAS operating system doesn't protect a vulnerable media server port-forwarded beside it. **Commands:** none were sourced, so none are given.

EXPLOITED · CISA KEV

## Three more on a three-day KEV clock

04

KEV 9 Nov · due 12 Nov | FreeSWITCH · GPUStack · IBM Aspera Faspex | Evidence: medium–strong

CONFIRMED On 9 November CISA added four CVEs: OpenSSH (article 1) and the three below. All four carry the unusually short **12 November** due date and a forensic-triage flag, and each required action cites "CISA's BOD 26-04 Prioritizing Security Updates Based on Risk" and "Forensics Triage Requirements". There were no additions on 7, 8 or 10 November as of catalog v2026.11.09. ↗ CISA KEV MAG212 ANALYSIS The three-day deadline appears to pair with the forensic-triage flag; we could not read the directive itself.

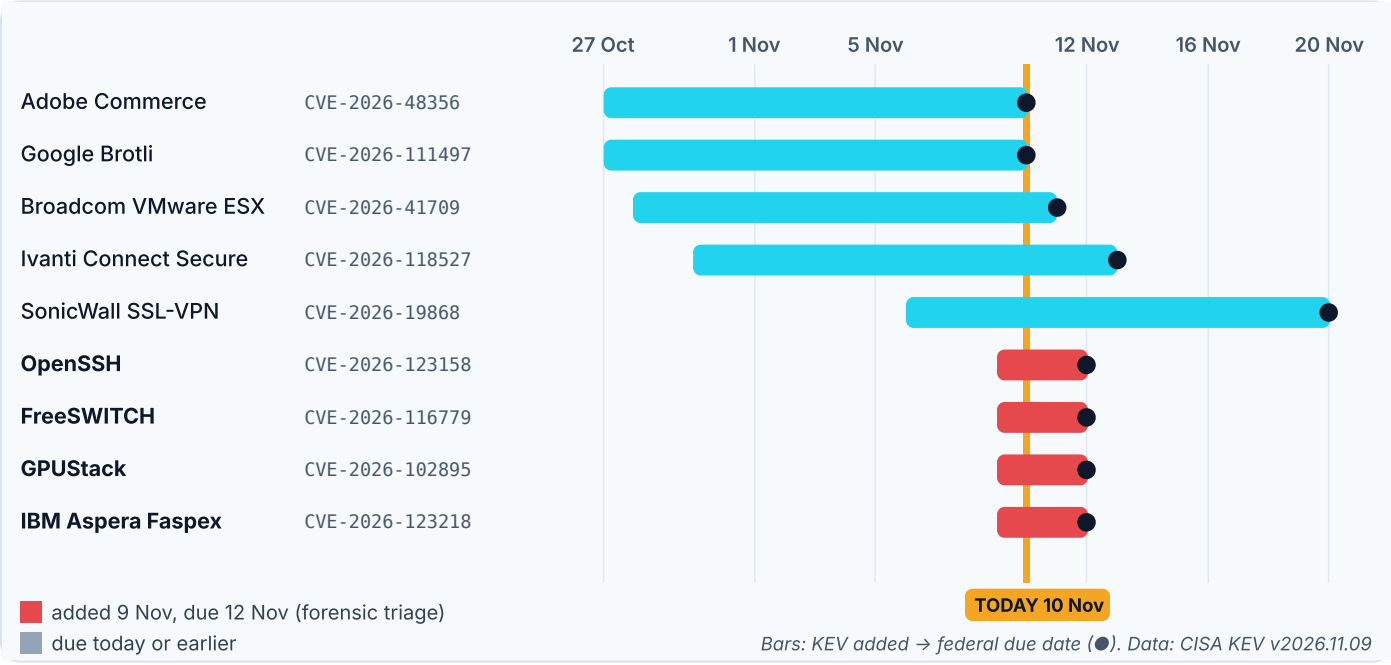



**Figure 4 · KEV clocks running this week.** Each bar runs from the date CISA added the flaw to KEV to the federal due date. The four 9 November additions (red) got three days.
*MAG212 CYBER original chart. Data: CISA KEV catalog v2026.11.09 (GitHub mirror).*

## FreeSWITCH: SIP MESSAGE command injection (CVE-2026-116779)

CONFIRMED KEV says it "permits configuration and credential disclosure, arbitrary call control, and command execution". ↗ CISA KEV REPORTED CVSS 9.8; affects 1.11.2 and earlier; fixed in **1.11.3**. The vendor advisory (GHSA-mg63-h38w-8p9p, 28 Oct) states "Exploitation of this path has been observed in the wild." An inbound SIP MESSAGE reaches the "api" chat handler and runs commands with server privileges. Chat is on by default for internal and external profiles, authenticating a MESSAGE needs only one account on the profile, and older sample configs include a directory user with no password. ↗ SecurityOnline

**Look for** unexpected SIP MESSAGE traffic and API activity in logs. **Remediate, in order:** upgrade to 1.11.3; keep `enable-chat-api-proto` off (default); set `enable-chat=false` where SIP chat isn't needed; remove passwordless directory users; set `ice_verify_message_integrity`; leave mod_xml_rpc `enable-websocket` unset. ↗ SecurityOnline UNKNOWN Who is exploiting it and which PBX products embed vulnerable FreeSWITCH. The vendor advisory was not opened by MAG212.

## GPUStack: improper authentication (CVE-2026-102895)

CONFIRMED KEV: "unauthenticated administrative access... persistent administrator API-key creation, disclosure of worker and cloud-provider secrets, and code execution through POST /v2/inference-backends/from-yaml". ↗ CISA KEV

REPORTED CVSS 9.8. Builds before 2.2.0 trust loopback requests as admin because `force_auth_localhost` defaults to false; attackers reach this through a same-host reverse proxy or a spoofed `X-GPUStack-Real-IP: 127.0.0.1` header. Exploitation was observed against v2.1.1, with custom backends used to launch reverse shells. Fixed in 2.2.0; **upgrade to 2.2.2 or later** to also fix SAML bypass CVE-2026-102894. Workarounds: `force_auth_localhost=true`, strip `X-GPUStack-Real-IP` at the proxy, block `/auth/saml/callback`. ↗ SecurityOnline MAG212 ANALYSIS Because cloud-provider and worker secrets are exposed, patching isn't enough on any exposed instance: rotate those credentials too.

## IBM Aspera Faspex: incorrect authorization (CVE-2026-123218)

CONFIRMED Affects Faspex 5.0.0 to 5.0.19; fixed in **5.0.19 PL1**; after patching, the faspex-core image should report "5.0.19 (1ce4b13, Fix Pack: 1)". IBM offers no workarounds and its bulletin does not mention exploitation. ↗ IBM KEV describes it as letting "an authenticated user... bypass authorization, causing privilege escalations". ↗ CISA KEV

**Conflict:** IBM scores it CVSS 9.8 with vector `PR:N` (no privileges required), which contradicts the "authenticated user" wording in both IBM's bulletin and KEV. The bulletin's "modified" date (6 Nov) also precedes its first-published date (7 Nov). MAG212 ANALYSIS Until IBM clarifies, treat it as needing no privileges and patch internet-facing Faspex first. UNKNOWN Who exploited it and how; the KEV listing is the only exploitation evidence.

Commands: none of the three sources supply shell commands; the settings above are configuration directives from the sources.

CLOUD & IDENTITY · OBSERVED IN THE WILD

05

# Qubole's own AWS account was turned on its customers

Observed in the wild | Reported 9 Nov · activity 8–26 Oct | Primary research not opened | Evidence: medium

| VENDOR | ABUSED | TARGET | VICTIMS |
|---|---|---|---|
| Qubole (data lake platform, owned by Idera) | AWS account 805246085872 | Customer IAM roles trusting Qubole | "Multiple" · no count |

## What happened

REPORTED An attacker holding credentials for **Qubole's AWS account (805246085872)** assumed IAM roles that customers had created to trust it, and the AssumeRole requests carried the correct External ID. Most of the roles were no longer used but still trusted Qubole. Sentra spotted the activity in several customers' environments and alerted Wiz. Neither Qubole nor Idera had made a public statement when The Hacker News checked. ↗ The Hacker News (primary research: Wiz, not opened by MAG212)

REPORTED TIMELINE AssumeRole break-ins ran **14–26 October**; from 18 October the attacker used IAM user `AIDAJYRRH5Y3A7AAJM2HW`. Separately, on **8–11 October**, an attacker not linked to the first used customers' own AWS access keys, an access option Qubole supports. ↗ The Hacker News

## Who is affected

Any AWS account containing an IAM role that trusts Qubole's account, **including roles nobody uses any more.**

REPORTED Qubole's setup guide includes a sample S3 policy that lets the role read every bucket in the account.

↗ Qubole docs

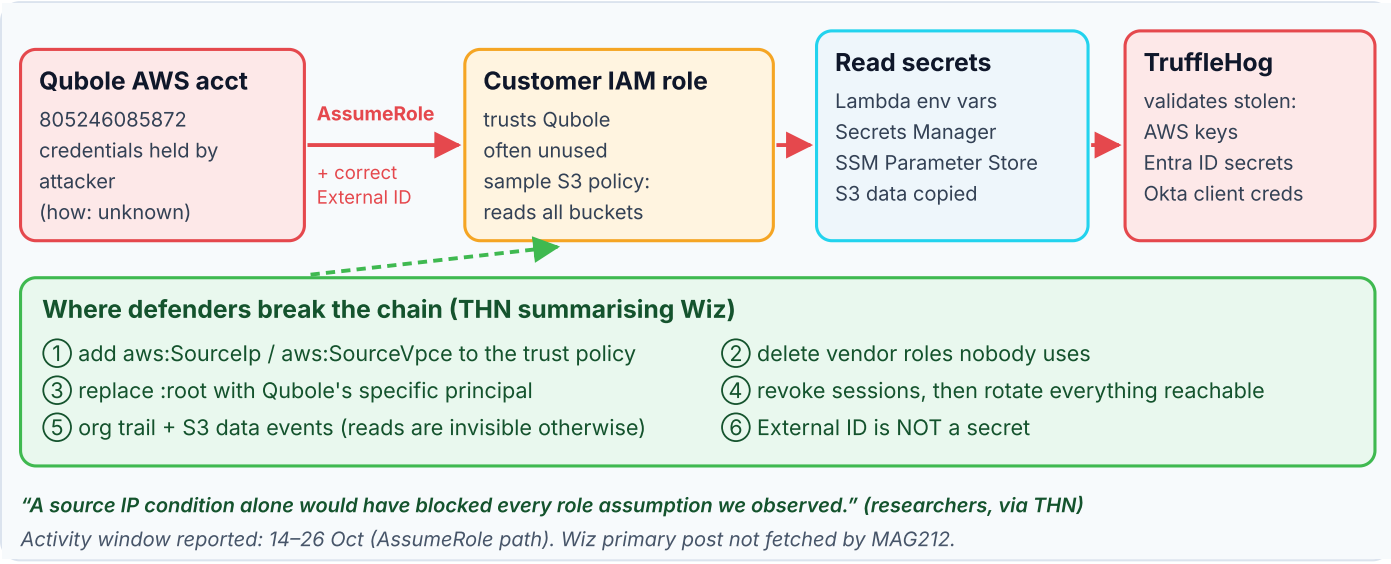



**Figure 5 · Qubole cross-account role abuse, and where to break it.** The reported chain from Qubole's AWS account to stolen cloud and identity secrets, with the six controls that would have stopped or exposed it.
*MAG212 CYBER original diagram, based on The Hacker News summarising Wiz research (9 Nov 2026). Wiz's post was not opened by MAG212.*

## How the attack works

REPORTED (1) AssumeRole into the customer role from Qubole's account; (2) read Lambda environment variables, Secrets Manager secrets and SSM Parameter Store values; (3) test the harvested credentials with TruffleHog, including victims' AWS keys, **Entra ID client secrets and Okta client credentials**; (4) copy S3 data, sometimes a whole bucket in one session. ↗ The Hacker News UNKNOWN How the attacker got Qubole's credentials, the number of victims, and whether a vendor statement will follow.

## What to look for (published indicators)

| Indicator | Context |
|---|---|
| Account `805246085872` | Flag AssumeRole calls from non-AWS IP addresses |
| `AIDA3W7DIFLYOLTK63SFS` | Used only by the attacker in the examined accounts: investigate all its activity |
| `AIDAJYRRH5Y3A7AAJM2HW` | Also used legitimately by Qubole: investigate only when the source is outside AWS |
| `57.129.54[.]120` , `2001:41d0:70d[:]7800::` | OVH |
| `45.83.220[.]211` , `185.209.199[.]73` , `89.37.63[.]175` | Mullvad shared VPN exits: not proof on their own |
| Session names `quiam-*` | Attacker role-session naming, e.g. `quiam-enum` |
| TruffleHog user agent | On `GetCallerIdentity` : credential validation |

Source: The Hacker News, summarising Wiz. Defanged with [.] and [:].

## Investigate, contain and remediate (in order)

1. Review **CloudTrail from 1 October** in every account holding a Qubole role.
2. **Revoke active sessions** for any abused role; rotation alone doesn't end them.
3. **Rotate everything the role could reach**, including Entra ID and Okta app credentials stored in AWS.
4. **Remove vendor roles you don't need.**
   Where Qubole supports it, replace the `:root` principal with Qubole's specific principal.

6. Add an `aws:SourceIp` or `aws:SourceVpce` condition. The researchers: "a source IP condition alone would have blocked every role assumption we observed."
7. Enable an **organization trail** and **S3 data events or server access logs**; management events don't show object reads.

Source for all steps: The Hacker News. Wiz's exact detection queries could not be verified, so none are reproduced.

## Verify recovery

Confirm no Qubole-trusting role remains without a source condition, that rotated secrets are the ones in use, and that S3 data-event logging is active.

## Prevention and awareness

REPORTED Don't treat the External ID as a secret. ↗ AWS guidance MAG212 ANALYSIS For MSPs, today's job is an inventory of vendor cross-account roles across every client AWS account, each with an owner and a reason to exist.

CRITICAL INFRASTRUCTURE · NATION-STATE

06

# France blames Iran's IRGC for heating supermarket fridges

Sabotage occurred | Statements 9 Nov · published 10 Nov | US advisory 5–6 Nov (background) | Evidence: medium

## What happened

REPORTED Paris prosecutors said Iran's Revolutionary Guard was behind the October attack on supermarket refrigeration, and France's cyber agency ANSSI attributed it to the **Shahid Kaveh group**, which it describes as an IRGC-affiliated cyber unit. Prosecutor Laure Beccuau opened a judicial investigation into organised cybercrime "aggravated by serving a foreign power, in this case, Iran", targeting the group's leader and two deputies. Cited evidence includes Farsi use and IP addresses linked to devices in Iran. International arrest warrants are being sought but not yet issued. Foreign minister Jean-Noël Barrot summoned Iran's ambassador and said France would seek sanctions "at the European level". ↗ SecurityWeek/AP

REPORTED IMPACT Attackers took control of refrigeration in about **700 of France's 10,000 supermarkets**; temperatures reached **50°C for about six hours**; Intermarché reported losses of "tens of millions of euros" in a day. ↗ SecurityWeek/AP AP dates the attack to 12 October; earlier reporting says overnight 11–12 October, which we use. ↗ SecurityWeek

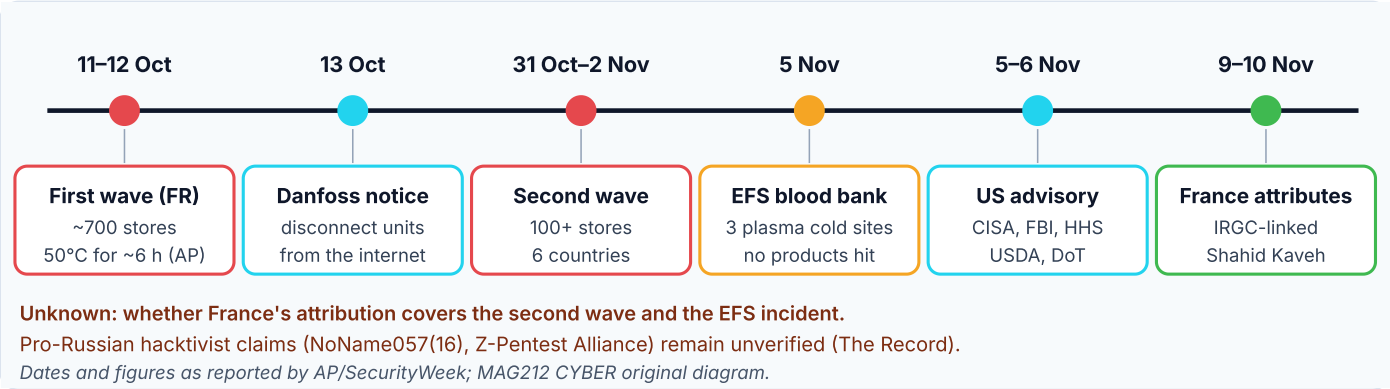



**Figure 6 · The refrigeration attacks, October–November.** From the first French wave to France's attribution. Whether the second wave and the EFS incident share an actor is unknown.
*MAG212 CYBER original timeline. Dates and figures as reported by AP/SecurityWeek and The Record.*

**Attribution conflict.** France's attribution is official. Earlier, pro-Russian hacktivists NoName057(16) and Z-Pentest Alliance reportedly claimed to have hacked Danfoss ↗ SecurityWeek; The Record calls those claims unverified. ↗ The Record UNKNOWN Whether the attribution covers the second wave (overnight 31 Oct–2 Nov, 100+ stores in Belgium, Estonia, Ireland, Luxembourg, the Netherlands and Sweden) and the French blood bank (EFS) incident, where attackers reached three plasma cold-storage sites through supplier Coolworld and EFS says "no blood products or samples were compromised". ↗ SecurityWeek ↗ SecurityWeek/AP Iran's response has not been reported.

## Who is affected

REPORTED CISA, FBI, HHS, USDA and DoT said they are "aware of malicious cyber actors targeting electronic temperature controllers and commercial refrigeration controllers in retail grocery and cold storage facilities". ↗ SecurityWeek (advisory PDF not opened by MAG212). CERT-FR first flagged Danfoss AK-SM and AK-SC controllers, then Copeland/Dixell XWEB. Danfoss said most hacked units were legacy products it no longer updated, and told customers on 13 October to disconnect them from the internet. ↗ SecurityWeek

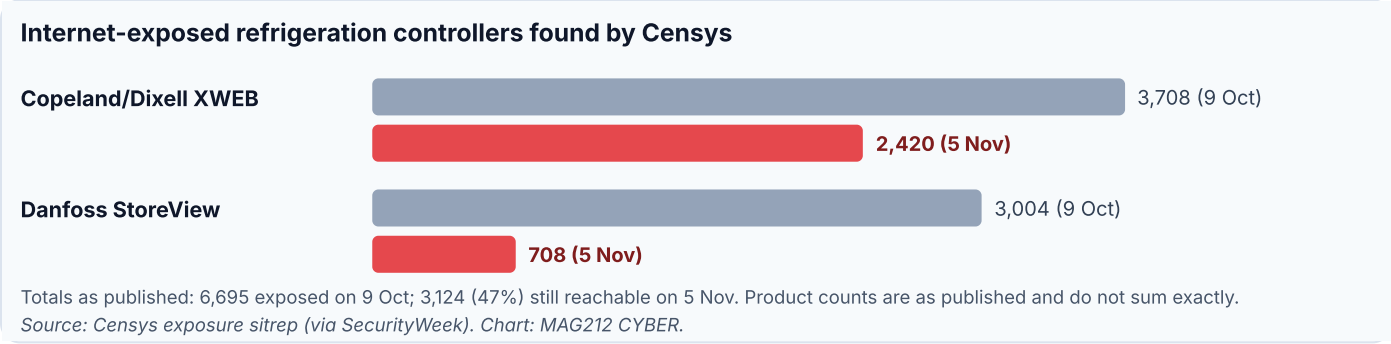



**Figure 7 · Exposed refrigeration controllers fell, but not enough.** Censys counts of internet-reachable controllers on 9 October and 5 November. Nearly half were still reachable after the first attacks.
*MAG212 CYBER original chart. Data: Censys exposure sitrep, via SecurityWeek. Product counts as published.*

## How the attack works and what to look for

REPORTED ADVISORY TTPS Attackers exploit unpatched or internet-accessible controllers through authentication bypass, code injection and weak configurations; remotely change settings to **force continuous heating and defrost cycles**; and cause **denial-of-view** so operators can't see the real state. ↗ SecurityWeek Look for unexplained setpoint or defrost changes and loss of visibility on controller dashboards. No IOCs were obtained because the advisory PDF was not retrieved.

## Contain, remediate and verify (in order)

1. **Take control systems off the internet**, or put them behind a firewall or edge device.
2. Isolate OT networks.
3. Restrict access to trusted identities, with strong passwords and **phishing-resistant MFA**.
4. Patch, or replace legacy controllers the vendor no longer updates.
5. Keep offsite backups of configurations; turn on logging and monitoring. ↗ SecurityWeek

**Verify recovery:** confirm from outside your network that controller interfaces no longer answer, and check setpoints against known-good values.

## Prevention and awareness

MAG212 ANALYSIS The official attribution turns a facilities problem into nation-state OT sabotage. MSPs serving retail, food, pharmacy or healthcare should treat any internet-reachable building controller as an incident waiting to happen. Related background: the CVSS 10 Node-RED flaw CVE-2026-58115 (Siemens SIMATIC IoT2050), which VulnCheck has seen exploited since 30 October through a single HTTP request against instances without adminAuth. ↗ SecurityWeek

DATA BREACH · EDUCATION

# Frontline Education breach doubles to 3.08 million

07

Updated 9 Nov | Not confirmed ransomware · unclaimed | Evidence: medium

| AFFECTED | EARLIER FILINGS | DETECTED | ENTRY |
|---|---|---|---|
| 3,085,266 people (Indiana AG filing) | about 1.3 million | 14 Aug · contained next day | Unnamed third-party software flaw |

## What happened and who is affected

REPORTED Frontline Education told the Indiana Attorney General's Office that **3,085,266 people** were affected, more than twice the roughly 1.3 million in its earlier state filings. Attackers exploited a vulnerability in an **unnamed third-party software product** and stole data from **Frontline Central and School Health Management**. Those affected are school district employees and students. Depending on the person, data may include names, SSNs, dates of birth, driver's licence, passport or other ID numbers, health insurance information such as Medicaid IDs, and student IDs. Frontline offers two years of credit monitoring for US adults and dark-web monitoring for eligible minors. No group has claimed the attack. ↗ SecurityWeek UNKNOWN Which third-party product was exploited.

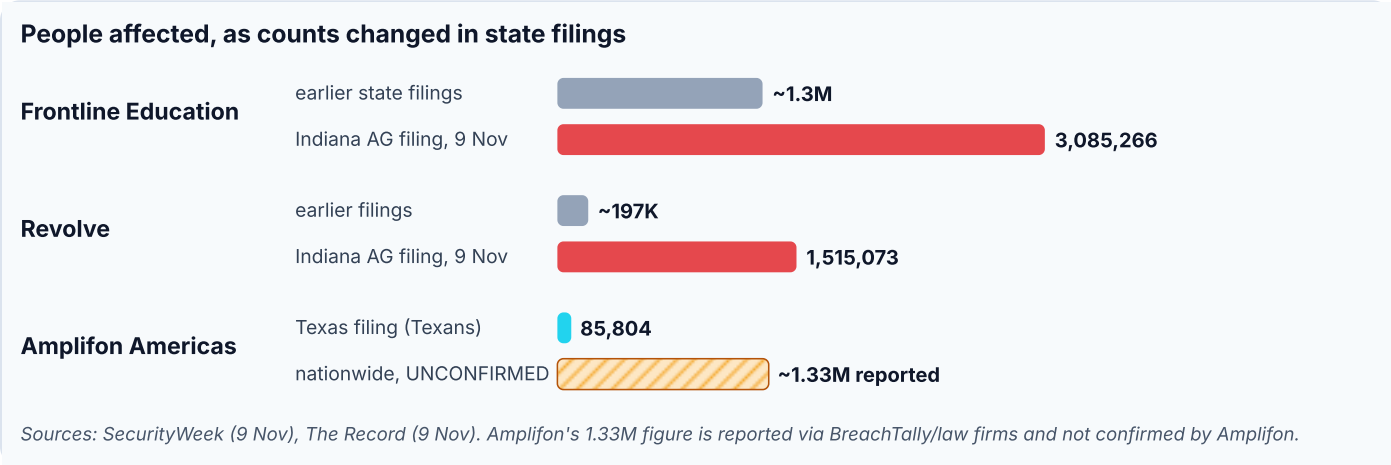



**Figure 8 · Counts grew in late state filings.** Frontline and Revolve counts rose sharply in Indiana filings. Amplifon's 1.33 million is hatched because Amplifon has not confirmed it.
*MAG212 CYBER original chart. Data: state AG filings as reported by SecurityWeek and The Record (9 Nov 2026).*

## What school IT teams should do

Guidance inferred from the reporting, not stated by Frontline. There are no IOCs, commands or technical fixes here, because the compromise is on the vendor's side.

1. Confirm your district's notification status with Frontline.
2. Prepare communications for parents and staff, and promote the free monitoring.
3. **Warn staff and families about phishing that uses the leaked data** (see the awareness lesson).
4. Ask your SaaS vendors which third-party components they rely on and how fast they patch them.

## Same-day updates: Amplifon and Revolve

**Amplifon Americas** (hearing healthcare). REPORTED Attackers copied files between 18 January and 8 February 2026; Amplifon noticed suspicious activity on 11 February. ↗ The Record Data includes government ID numbers, dates of birth, hearing and medical information and health insurance information; SSNs and financial information for some people. Amplifon says it knows of no misuse. ↗ SecurityWeek

**Conflicting count.** The Texas filing lists **85,804 Texans** (plus 1,027 in Vermont). ↗ The Record A nationwide figure of about **1.33 million** has been reported, sourced through BreachTally and class-action law firms, but **not confirmed by Amplifon**. ↗ SecurityWeek ↗ BreachTally

**Revolve** (fashion e-commerce). REPORTED Revolve told the Indiana AG that **1,515,073 people** were affected, up from about 197,000 in earlier filings. The intrusion happened on 11 September and Revolve learned of it on 29 September. Card numbers and expiry dates were exposed for customers with stored payment methods; the way in is undisclosed. ↗ SecurityWeek

MAG212 ANALYSIS None of these is confirmed ransomware or claimed, so we call them data breaches. In all three, the real scale surfaced weeks or months later in state filings: treat early counts as provisional.

SOFTWARE SUPPLY CHAIN

08

# Signed, provenanced and malicious: bee-js and Swarm Desktop

Malicious releases shipped | Socket research 9 Nov, 14:52 UTC | Evidence: strong

| MALICIOUS | SAFE | NPM WINDOW | ASSESSED ACTOR |
|---|---|---|---|
| @ethersphere/bee-js 13.3.0 (npm) · Swarm Desktop 0.56.2 | bee-js 13.2.0 · Desktop 0.56.3 (unconfirmed at 10:30 UTC) | ≈75 minutes on 9 Nov | Same as SleepyDuck/EtherDuck (Socket) |

## What happened and who is affected

CONFIRMED Compromised maintainer accounts pushed malicious **@ethersphere/bee-js 13.3.0** to npm and **Swarm Desktop 0.56.2** as a GitHub release for Linux, macOS and Windows. npm removed 13.3.0 about 75 minutes after publication; 13.2.0 is the safe version. The 0.56.2 tag was deleted at 09:04 UTC on 9 November; 0.56.3 is recommended but had not been published as of 10:30 UTC. ↗ Socket ↗ The Hacker News Socket assesses the actor as the one behind the SleepyDuck/EtherDuck Open VSX campaign, based on on-chain history, shared payload hashes and identical persistence names. UNKNOWN How the GitHub accounts were compromised, download counts for 13.3.0, and whether Ethersphere has published its own advisory.

## How the attack works

CONFIRMED The attacker used `nugaon`, a maintainer with force-push rights to an unprotected `master`, and `bee-worker`, the release bot. In bee-js, unsigned commit `de2f74e` turned `scripts/generate-version.cjs` into a loader and renamed `prepare` to `postinstall`; a GitHub release then triggered the legitimate publish workflow, whose environment had no required reviewers and no tag policy, so npm provenance is valid. In Swarm Desktop, unsigned branch `emergency/0.56.2` added the loader, and a manually dispatched `pre-release.yml` that accepts any branch and holds Apple and Windows signing certificates built, signed and notarized the trojanized app. ↗ Socket

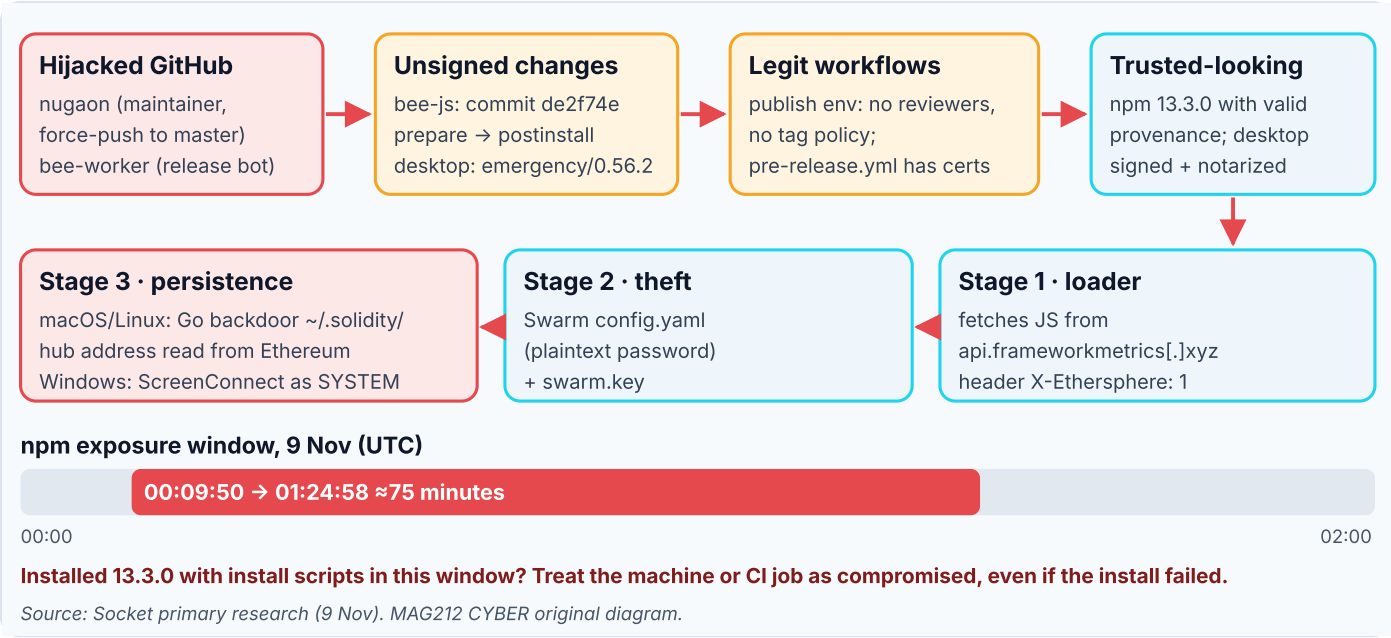



**Figure 9 · From hijacked accounts to signed malware.** Legitimate release workflows turned unsigned attacker changes into a validly provenanced npm package and a signed, notarized desktop app. The bar shows the npm exposure window.
*MAG212 CYBER original diagram, based on Socket's primary research (9 Nov 2026).*

## What to look for (published indicators)

| Type | Indicator (defanged) |
|---|---|
| Package | `@ethersphere/bee-js@13.3.0` · tarball SHA-256 `d01fdf241aa9e0a1ba6ebc19f8f667af1bf652745021c5050126cb7036f7ce58` |
| Domain | `api.frameworkmetrics[.]xyz` (registered 6 Nov) |
| Hubs, port 4912 | `193.57.9[.]155` (current), `193.57.9[.]17`, `178.16.54[.]222`, `107.189.27[.]223`, `107.189.27[.]46`, `91.108.240[.]156`, `107.189.16[.]215` |
| Payload URL | `hxxp://107.189.27[.]46:3000/app.js` |
| ScreenConnect relay | `185.232.84[.]169:8041` |
| Ethereum contracts | `0xf8a900Db50b3331be6B768bA460BB59f3E40C344` (eth_call data `0x02d91518`) · `0x6a82595EEea0f4FDFB3aE13A2687BcbBE626e94B` |
| Persistence | `~/.solidity/` · `solidity-langsupport-runner.service` · `com.solidity.langsupport.runner` · service `ScreenConnect Client (5cbe79c9c25524df)` |
| SHA-256 | `generate-version.cjs` ee2f762e9ed3fd89f106e0b80c2e923bf1aed9a280277d3d998a5902c4d9ec0f · desktop `index.js` f81315968e679b48f6bdff1c9b928bb223230d07f44d7948412c2250c2a14deb · stage 3 darwin_arm64 fae61f31f00988fdc5cc9e7272b51e08af2e245d81003237875415930fd27358 · stage 3 linux_amd64 9b73e7cd4e1425e770392549d8df46c706139ef476f4f7b9ac405165dc8d9696 · `invoke.ps1` 37d14bff30762ca701e9c1f8bc6c57c065bb20ae3a2208cb7411a6530610f08e |
| Log string | `Bee Desktop version: 0.56.2 (production)` in `bee-desktop.log` |

Source: Socket, which also lists commit hashes and the npm integrity string.

## Investigate, contain and remediate (in order)

1. Search lockfiles, caches and internal registries for 13.3.0; pin 13.2.0 and purge mirrors.
2. Treat any machine or CI job that installed 13.3.0 with install scripts enabled **between 00:09:50 and 01:24:58 UTC on 9 November** as compromised, **even if the install failed**.
3. Rotate every credential those machines or jobs could reach, including CI OIDC-trusted cloud credentials.
4. Swarm Desktop users: assume the node password and key are stolen and **move funds to a new key from a clean machine**.
5. **Manually remove** `~/.solidity/`, the LaunchAgent, the systemd unit and the ScreenConnect service; reinstalling does not remove them.

6 Hunt in DNS and proxy logs for the domain and IPs above. ↗ Socket

### Verify recovery

Confirm lockfiles resolve to 13.2.0, the persistence artefacts are gone, and nothing still connects to the hub or relay addresses.

### Prevention and awareness

SOCKET'S ADVICE Verify a released commit sits on a protected branch or came from a merged release PR; require reviewers on publish environments and restrict which tags can deploy; don't expose signing credentials to manually dispatched workflows; scope and rotate release-bot tokens. ↗ Socket MAG212 ANALYSIS Valid provenance and notarization prove which pipeline built the code, not that the code is benign. Direct impact is probably limited to Swarm and Ethereum users, but the CI/CD lesson applies to anyone who publishes software, and it fits GitHub's announced change to block `pull_request_target` workflows by default from 2 December. ↗ Socket

## Defender's Action Desk

A prioritised checklist built from today's stories. Tick what applies to your estate; skip what doesn't.
MAG212 ANALYSIS for the ordering; each action's source is in its article.

- [ ] NOW **Alpine/musl sshd:** `PasswordAuthentication no`, upgrade `openssh`, restart sshd, grep `/var/log/messages` for `Accepted password for` on passwordless accounts. → 01
- [ ] NOW **SonicWall:** upgrade to 7.3.4-7013 / 8.2.3-8015, SAML SSL-VPN portals first; restrict the management interface. → 02
- [ ] NOW **NAS:** close port 32400, turn off Plex Remote Access, reinstall Plex 1.43.3.10861+, rotate passwords. → 03
- [ ] NOW **bee-js:** search lockfiles for 13.3.0; treat installs in the 9 Nov window as compromised; rotate CI credentials. → 08
- [ ] TODAY **AWS:** list roles trusting vendor accounts (start with `805246085872`); delete unused; add `aws:SourceIp` / `aws:SourceVpce`; CloudTrail from 1 Oct. → 05
- [ ] TODAY **FreeSWITCH / GPUStack / Faspex:** 1.11.3 · 2.2.2+ · 5.0.19 PL1; rotate GPUStack cloud and worker secrets. → 04
- [ ] TODAY **Building & OT controllers:** check from outside that refrigeration and other controllers aren't internet-reachable. → 06
- [ ] THIS WEEK **Schools:** confirm Frontline notification status; send the phishing warning in the awareness lesson. → 07
- [ ] THIS WEEK **CI/CD:** require reviewers on publish environments; keep signing secrets away from manually dispatched workflows. → 08
- [ ] THIS WEEK **AI coding tools:** scan `.claude/`, `.cursor/`, `.gemini/`, `.specstory/` for committed secrets (Briefly noted).

### KEV deadlines falling this week

| CVE | Product | Added | Federal due date |
|---|---|---|---|
| CVE-2026-48356 | Adobe Commerce | 27 Oct | **10 Nov (today)** |
| CVE-2026-111497 | Google Brotli | 27 Oct | **10 Nov (today)** |
| CVE-2026-41709 | Broadcom VMware ESX | 28 Oct | 11 Nov |
| CVE-2026-123158 | OpenSSH | 9 Nov | 12 Nov |
| CVE-2026-116779 | FreeSWITCH | 9 Nov | 12 Nov |

| CVE | Product | Added | Federal due date |
|---|---|---|---|
| CVE-2026-102895 | GPUStack | 9 Nov | 12 Nov |
| CVE-2026-123218 | IBM Aspera Faspex | 9 Nov | 12 Nov |
| CVE-2026-118527 | Ivanti Connect Secure | 30 Oct | 13 Nov |
| CVE-2026-19868 | SonicWall SonicOS SSLVPN | 6 Nov | 20 Nov |

Source: CISA KEV catalog v2026.11.09. Federal deadlines apply to US agencies, but they're a useful priority signal for everyone. Related: Singapore's CSA updated its alert on exploited Cisco ASA/FTD SSL VPN reload flaw CVE-2026-76418 (KEV since 29 Oct) on 10 Nov. ↗ CSA Singapore

### ⏳ Watch today: not confirmed at the research cutoff

- **Microsoft Patch Tuesday** was not published. We give no counts or zero-days until the MSRC Update Guide is live. Separately, Microsoft Entra Device Registration CVE-2026-109469 (CVSS 10.0) was listed on 7 Nov as already mitigated by Microsoft, with no customer action and no exploitation. ↗ Oflight
- **Fortinet** patched critical flaws in FortiOS, FortiManager, FortiAnalyzer, FortiMail and FortiAuthenticator on 21–22 Oct and said it would publish CVE IDs by 10 Nov; not confirmed live. Fixed versions circulating come from a social post and are **unverified**. watchTowr expects rapid exploitation and advises taking internet-exposed management interfaces offline or restricting them; no exploitation is confirmed. ↗ Cybernews
- **Chrome:** a 10 Nov SecurityWeek headline reports an update fixing an exploited XML zero-day. We didn't read the article, so no version or CVE is given. ↗ SecurityWeek
- **ICS:** Siemens and Schneider advisories are likely today ( MAG212 ANALYSIS ); none verified. Latest confirmed CISA ICS advisory: ICSA-26-307-01 (3 Nov). ↗ CISA
- **Also open:** Swarm Desktop 0.56.3 release; G7 discussion of joint cyber measures (9–10 Nov); France's announced EU sanctions and arrest warrants. ↗ The Record

# Awareness lesson: "The breach letter is the bait"

### For employees, staff and families

Frontline (3.08 million school staff and students), Amplifon and Revolve are all sending breach notices this week. Expect phishing that quotes **real** personal details. ↗ SecurityWeek

- An email that knows your date of birth or employee ID is **not proof** it's genuine.
- Reach any monitoring offer only through your district's or employer's official site, never a link in an unsolicited message.
- Nobody legitimate needs your password or a one-time code to "verify" your monitoring.
- Not sure? Forward it to IT and delete it.

### For leaders and owners

This week's incidents all ran through something an organisation had deliberately trusted.

MAG212 ANALYSIS

**Ask your team for one page** listing standing vendor access, parallel login methods and internet-reachable management interfaces, each with a named owner and a reason it still exists.

Removing a trust nobody needs costs nothing, and it's the cheapest control in this issue.

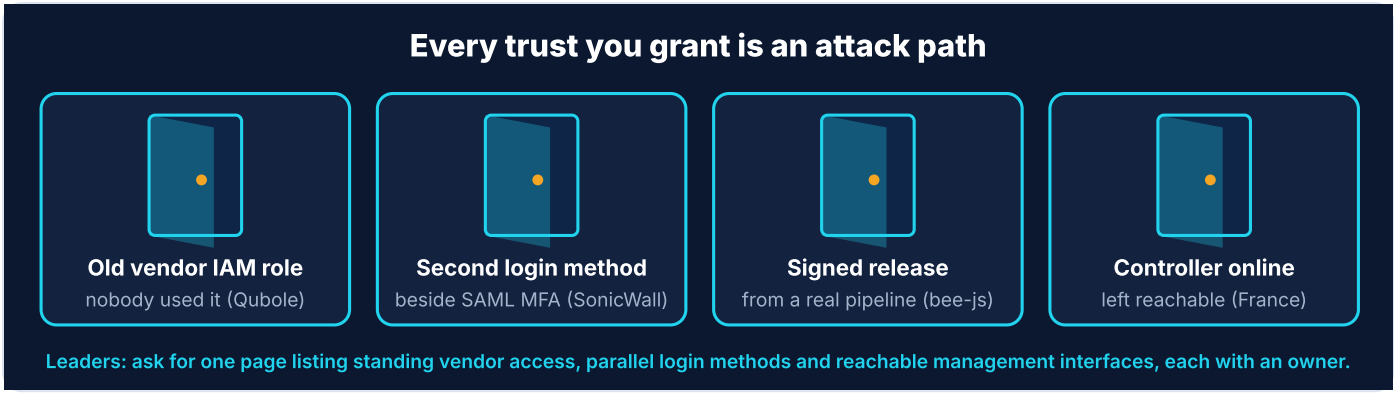



**Figure 10 · Four trusted doors used this week.** Each of this week's major incidents ran through access an organisation chose to grant. *Conceptual MAG212 CYBER original illustration.*

## Briefly noted

- **Claude Code secrets in public repos (7 Nov, ~3 days old).** REPORTED Apiiro found the "Yes, and don't ask again" option saves approved commands verbatim, including literal secrets, to `.claude/settings.local.json`. Of 104,185 public copies, 1,122 contain at least one secret (1,379 distinct); Gitleaks and TruffleHog missed 215 of those files. No Anthropic statement was reported; an earlier bug report was closed by a bot. ↗ The Hacker News ↗ Apiiro Rotate exposed secrets first, then untrack the file:

  **Untrack the file** OS: any Shell: any, inside the repo Privileges: none **CHANGE (git index only)**

  ```
  git rm --cached .claude/settings.local.json
  # then add .claude/settings.local.json to .gitignore and commit
  ```

  Removes the file from version control but keeps it on disk; history still contains old copies, so rotation comes first. Not tested by MAG212 CYBER; syntax from The Hacker News.

- **Iris Plaza (9 Nov):** a compromised external cloud service may have exposed data on 7.7 million customers; article not read in full. ↗ SecurityWeek
- **NoName057(16) doxxing (9 Nov):** personal data of 18 European officials and journalists, including Italy's foreign minister Antonio Tajani, published with crypto bounties; the Russian Embassy denied involvement. ↗ The Record
- **Ukraine arrests (9 Nov):** four people held over a call-centre investment scam that took more than €4.3M from 135 German victims. ↗ The Record
- **AI and attackers (9 Nov):** an attacker used BOSSAI agents against Taipei emergency dispatch records ↗ The Hacker News; Google DeepMind agents lowered the cost of attacking RSA-1024 ↗ SecurityWeek.

# Source register

Every source behind this issue; each title links to the source. "Opened" means our research team read it; "No" means it could not be reached and claims from it rest on the secondary sources listed. All links checked for correct form; we did not re-fetch them at publication. Editorial method: original summaries and analysis, short attributed quotes only. Corrections: write via cyber.mag212.com.

| # | Publisher / title | Date | Type | Opened? | Site |
|---|---|---|---|---|---|
| 1 | CISA KEV catalog (GitHub mirror, v2026.11.09) | 9 Nov 2026 | Primary (government) | Yes | raw.githubusercontent.com |
| 2 | OpenSSH release notes (10.6p2) | 5 Nov 2026 | Primary (vendor) | Yes | openssh.org |
| 3 | Alpine Linux: OpenSSH password authentication bypass | 5 Nov 2026 | Primary (vendor) | Yes | alpinelinux.org |
| 4 | Help Net Security: OpenSSH sshole exploitation | 6 Nov 2026 | Secondary | Yes | helpnetsecurity.com |
| 5 | SecurityWeek: Hackers exploiting SSHole | 9 Nov 2026 | Secondary | Listing | securityweek.com |
| 6 | SecurityWeek: OpenSSH rushes patches | Nov 2026 | Secondary | No | securityweek.com |
| 7 | The Hacker News: OpenSSH sshole exploited | Nov 2026 | Secondary | No | thehackernews.com |
| 8 | CIS advisory 2026-040 | Nov 2026 | Secondary (advisory) | No | cisecurity.org |
| 9 | HKCERT OpenSSH bulletin | 6 Nov 2026 | Secondary (CERT) | No | hkcert.org |
| 10 | BleepingComputer: SonicWall SSL-VPN MFA bypass | 6 Nov 2026 | Secondary | Yes | bleepingcomputer.com |
| 11 | SecurityWeek: SonicWall patches exploited SonicOS bug | 7 Nov 2026 | Secondary | Yes | securityweek.com |
| 12 | SonicWall PSIRT SNWLID-2026-0014 | 6 Nov 2026 | Primary (vendor) | No (timeout) | psirt.global.sonicwall.com |
| 13 | CISA alert: adds one KEV (SonicWall) | 6 Nov 2026 | Primary (government) | No (blocked) | cisa.gov |
| 14 | The Hacker News: CISA flags SonicWall MFA bypass | 9 Nov 2026 | Secondary | Listing | thehackernews.com |
| 15 | Oflight vulnerability digest | 7 Nov 2026 | Secondary | Yes | oflight.co.jp |
| 16 | SecurityWeek: Plex2Shell exploited against QNAP NAS users | 9 Nov 2026 | Secondary | Yes | securityweek.com |
| 17 | QNAP security notice: Plex2Shell | Nov 2026 | Primary (vendor) | Not confirmed | qnap.com |
| 18 | QNAP FAQ: Plex2Shell check and remediation | Nov 2026 | Primary (vendor) | Not confirmed | qnap.com |
| 19 | SecurityOnline: FreeSWITCH CVE-2026-116779 exploited | 29 Oct 2026 | Secondary | Yes | securityonline.info |
| 20 | FreeSWITCH GHSA-mg63-h38w-8p9p | 28 Oct 2026 | Primary (vendor) | No (timeout) | github.com |
| 21 | SecurityOnline: GPUStack CVE-2026-102895 exploited | 5 Nov 2026, updated 10 Nov | Secondary | Yes | securityonline.info |
| 22 | IBM security bulletin: Aspera Faspex | 7 Nov 2026 | Primary (vendor) | Yes | ibm.com |
| 23 | The Hacker News: Qubole trusted AWS access abused | 9 Nov 2026 | Secondary | Yes | thehackernews.com |
| 24 | Wiz: Qubole cross-account access abused in the wild | ~9 Nov 2026 | Primary (researcher) | No (timeout) | wiz.io |
| 25 | Qubole docs: create IAM roles | n/a | Vendor documentation | Cited via THN | docs.qubole.com |
| 26 | AWS: External ID for third-party access | n/a | Vendor documentation | Cited via THN | docs.aws.amazon.com |
| 27 | SecurityWeek/AP: France blames Iran for refrigerator cyberattack | 10 Nov 2026 | Secondary (wire) | Yes | securityweek.com |
| 28 | SecurityWeek: US agencies urge hardening of refrigeration controllers | 6 Nov 2026 | Secondary | Yes | securityweek.com |

| # | Publisher / title | Date | Type | Opened? | Site |
|---|---|---|---|---|---|
| 29 | IC3 joint advisory 261105 (PDF) | 5 Nov 2026 | Primary (government) | No (timeout) | ic3.gov |
| 30 | Censys: European refrigeration controller exposure | Nov 2026 | Primary (researcher) | Cited via SecurityWeek | censys.com |
| 31 | SecurityWeek: Over 100 European stores hit as fridge attacks resume | 3 Nov 2026 | Secondary | Yes | securityweek.com |
| 32 | SecurityWeek/AP: French blood bank site hit | 5 Nov 2026 | Secondary (wire) | Yes | securityweek.com |
| 33 | SecurityWeek: Critical Node-RED flaw exploited | 3 Nov 2026 | Secondary | Yes | securityweek.com |
| 34 | CISA GovDelivery: ICSA-26-307-01 | 3 Nov 2026 | Primary (government) | Yes | content.govdelivery.com |
| 35 | The Record: Pro-Russian hackers target European officials (NoName) | 9 Nov 2026 | Secondary | Yes | therecord.media |
| 36 | SecurityWeek: Italy's Meloni blames pro-Russian hackers | 9 Nov 2026 | Secondary | Headline only | securityweek.com |
| 37 | SecurityWeek: 3 million people hit by Frontline Education breach | 9 Nov 2026 | Secondary | Yes | securityweek.com |
| 38 | SecurityWeek: Amplifon Americas breach impacts 1.3 million | 9 Nov 2026 | Secondary | Yes | securityweek.com |
| 39 | The Record: Amplifon hearing aid company data breach | 9 Nov 2026 | Secondary | Yes | therecord.media |
| 40 | BreachTally: Texas AG record BR-0005495 | Nov 2026 | Tertiary aggregator | Cited via SecurityWeek | breachtally.com |
| 41 | Amplifon Americas security incident notice | 2026 | Primary (company) | No (blocked) | amplifonusa.com |
| 42 | SecurityWeek: Revolve puts breach victim count at 1.5 million | 9 Nov 2026 | Secondary | Yes | securityweek.com |
| 43 | Socket: bee-js compromise | 9 Nov 2026 | Primary (researcher) | Yes | socket.dev |
| 44 | The Hacker News: Ethersphere bee-js and Swarm Desktop compromised | 9 Nov 2026 | Secondary | Listing | thehackernews.com |
| 45 | Socket: GitHub to block pull_request_target | 5 Nov 2026 | Secondary | Listing | socket.dev |
| 46 | Cybernews: Fortinet critical flaws, November disclosure | Oct–Nov 2026 | Secondary | Yes | cybernews.com |
| 47 | CSA Singapore AL-2026-159 (Cisco ASA/FTD) | Updated 10 Nov 2026 | Government (CERT) | Yes | csa.gov.sg |
| 48 | Microsoft MSRC Update Guide | Pending | Primary (vendor) | Not yet published | msrc.microsoft.com |
| 49 | Help Net Security: October 2026 Patch Tuesday (CVE-2026-96951) | 14 Oct 2026 | Secondary | Search result | helpnetsecurity.com |
| 50 | SecurityWeek: Chrome update patches exploited XML zero-day | 10 Nov 2026 | Secondary | Headline only | securityweek.com |
| 51 | The Hacker News: Claude Code "don't ask again" file leaks secrets | 7 Nov 2026 | Secondary | Yes | thehackernews.com |
| 52 | Apiiro: coding agents leaking secrets | ~7 Nov 2026 | Primary (researcher) | No | apiiro.com |
| 53 | GitHub issue anthropics/claude-code #5544 | 11 Aug 2025 | Primary (issue tracker) | Cited via THN | github.com |
| 54 | SecurityWeek: Iris Plaza breach may have exposed 7.7M | 9 Nov 2026 | Secondary | Headline only | securityweek.com |
| 55 | The Record: Ukraine arrests scam call-centre operators | 9 Nov 2026 | Secondary | Yes | therecord.media |
| 56 | The Hacker News: Taiwan-based hacker used BOSSAI agents | 9 Nov 2026 | Secondary | Listing | thehackernews.com |
| 57 | SecurityWeek: DeepMind AI agents and RSA-1024 | 9 Nov 2026 | Secondary | Listing | securityweek.com |

# MAG212 CYBER

DAILY CYBER INTELLIGENCE

## Get tomorrow's briefing before your first coffee

Verified stories, the three actions that matter, and clear labels for what's confirmed, reported and still unknown. Free.

**Subscribe free →**

cyber.mag212.com/subscribe-free

**Verified, not viral**
Primary sources first, conflicts flagged, nothing invented.

**Built for defenders**
Versions, fixes, log locations and ordered remediation steps.

**For every team**
Network engineers, MSPs, school IT, IT managers and owners.

Editor: **El Mostafa Ouchen** · cyber.mag212.com · Issue MAG212_CYBER_Daily_2026-11-10