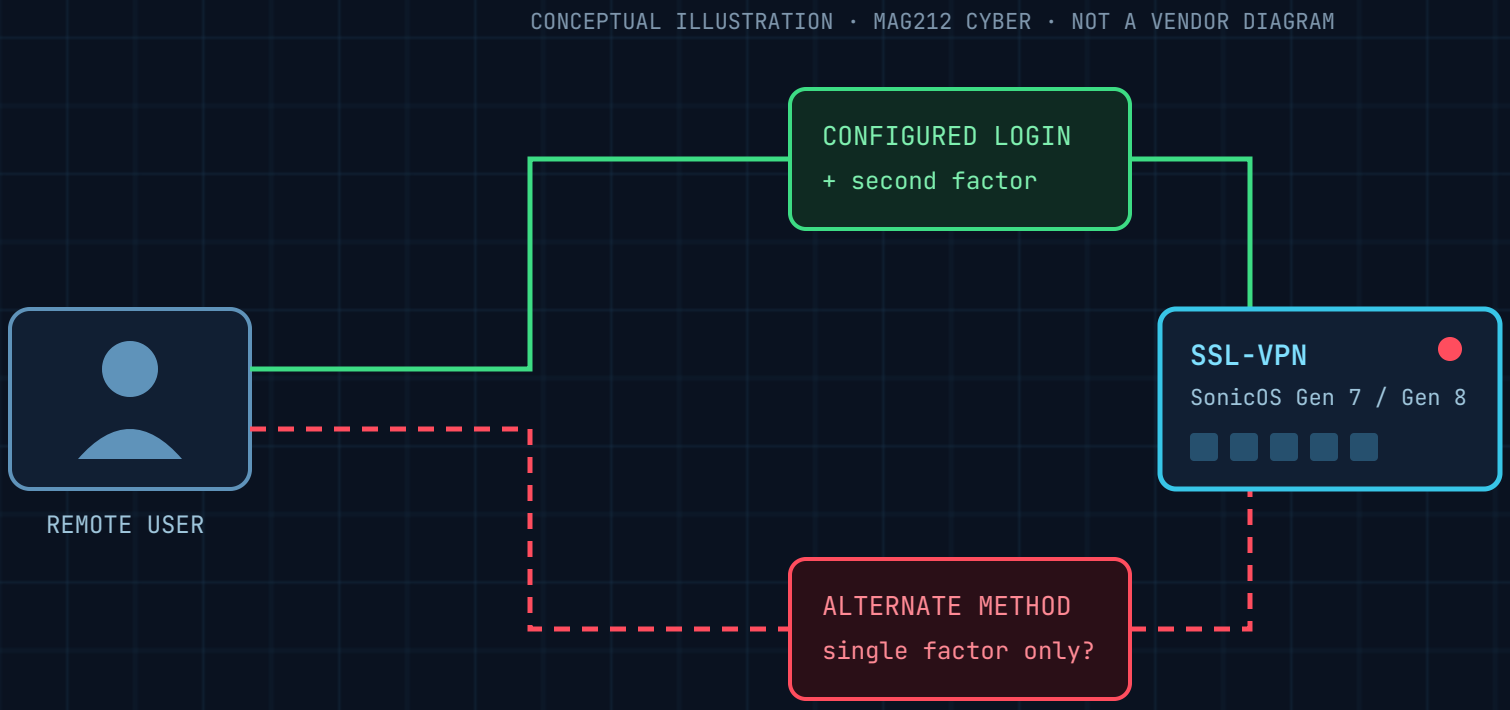
DAILY

SATURDAY · NOVEMBER 07 · 2026

MAG212 CYBER

DAILY CYBER INTELLIGENCE



SonicWall VPN flaw is now exploited

CISA added CVE-2026-19868 to its exploited list on Nov 6. Federal deadline: Nov 20. Here is what to patch, what to check, and what the advisory leaves unsaid.

BREACH
Chainalysis: every user's credentials and live tokens exposed

DEV SECURITY
Coding-agent approval files leak 1,379 secrets

MOBILE
APT29 hits unpatched phones via hacked websites

EXECUTIVE BRIEFING

What matters today

An exploited firewall VPN flaw, a security-data company that has to reset every customer's credentials, and a reminder that "approve forever" buttons write secrets to disk. Three actions for this shift:

1. **Patch SonicWall Gen 7 and Gen 8 firewalls**
   CVE-2026-19868 lets SSL-VPN logins skip the authentication you configured, via an alternate method. It is exploited and has a federal deadline of Nov 20. Install Gen 8 8.2.3-8015 or the newest Gen 7 7.3.4 build, then review VPN logins since late October.[1][5][6]

2. **Rotate Chainalysis credentials and API keys**
   Chainalysis now says names, usernames, password hashes and live tokens for **all** users were exposed. Reset passwords and rotate API keys once IP allowlisting is in place, and plan around offline KYT and Reactor services.[7][8]

3. **Scan repositories for agent approval files**
   Researchers found 1,379 secrets in public `.claude/settings.local.json` files. Look for tracked agent settings in your repos and their history, and rotate anything you find before cleaning up.[9][11]

> **How to read this issue.** Each story separates **confirmed facts** (vendor, government or original researcher), **reported claims** (credited to whoever made them) and **MAG212 analysis**. In diagrams, solid boxes are documented steps, dashed boxes are unknown, and green boxes are recommended defenses. Bracketed numbers link to the source register on page 19.

IN THIS ISSUE

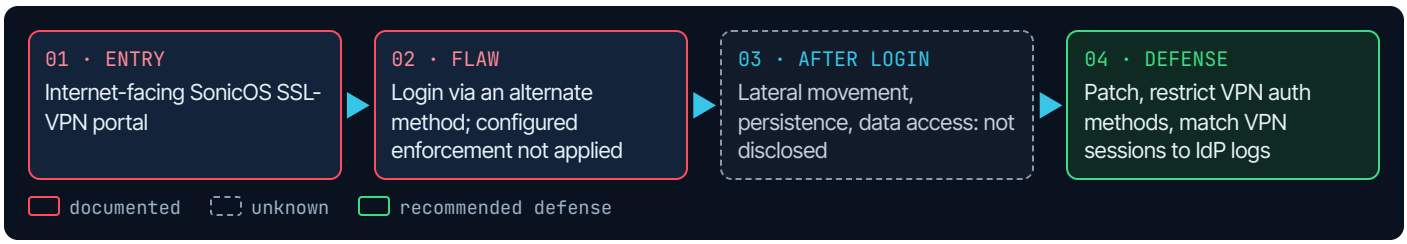
SonicWall VPN flaw exploited 03
Field guide: SonicOS patch & check 04
Deep dive: proving MFA was enforced 05
Chainalysis: all users exposed 06
Agent approval files leak secrets 07
Field guide: scan agent settings 08
SSHole update: attempts spread 09
Deep dive: inside the SSHole code path 10
WordPress: guard the first update 11
Deep dive: block, update, hunt 12
APT29 targets unpatched phones 13
Data exposure briefs 14
Policy & AI briefs 15
Defender's Action Desk 16
Awareness lesson & subscribe 17
Verification notes & sources 18

01 / EDGE AND IDENTITY EXPLOITED · KEV

SonicWall VPN logins can skip the checks you configured

A SonicOS SSL-VPN flaw lets users authenticate through an alternate method that doesn't enforce the configured policy. SonicWall says it is being exploited, and CISA has set a Nov 20 deadline for federal agencies.

CVE	KEV ADDED	AFFECTED	FIXED
CVE-2026-19868	Nov 6 · due Nov 20	Gen 7 ≤ 7.3.3-7015 · Gen 8 ≤ 8.2.2-8015	Gen 7 7.3.4 · Gen 8 8.2.3-8015



Steps 01–02 follow SonicWall's release-note wording and CISA's KEV entry. Nothing public describes what attackers did after logging in. Diagram: MAG212 CYBER. [2][6]

What happened

Confirmed: SonicWall published advisory SNWLID-2026-0014 on Nov 3 and updated it Nov 6. Canada's Cyber Centre (AV26-1133, Nov 6) says SonicWall "indicates that CVE-2026-19868 is being exploited." CISA's catalog data shows the CVE added on Nov 6 as a "Use of Single-factor Authentication" vulnerability in SonicOS SSLVPN, due Nov 20. Ransomware use is listed as unknown.[1][4][5][6]

The Gen 8 8.2.3-8015 release notes describe a fix titled "SSLVPN authentication enforcement vulnerability via alternate authentication methods." No public source we reached ties that line to the CVE number, but the wording and the KEV classification match.[2]

Who is affected

SonicWall lists Gen 7 SonicOS 7.3.3-7015 and older, and Gen 8 SonicOS 8.2.2-8015 and older. Gen 6 and older firewalls are past end of support and will not be patched; SonicWall points owners to its trade-in program.[1]

Version conflict: the Canadian advisory lists Gen 8 as affected "prior to 8.2.2-8015." SonicWall's own notice says 8.2.2-8015 is still affected. Go with the vendor: only 8.2.3-8015 is fixed.[1][5]

How the attack works

Based on the vendor wording and CISA's classification, an attacker can complete an SSL-VPN login through a secondary authentication method that does not apply the full policy, such as a required second factor. **Not confirmed:** whether SAML is involved, and whether valid credentials are needed. Treat both as unconfirmed until SonicWall publishes full CVE details.

Why it matters

MAG212 analysis: VPN appliances are a common first step into networks. If a flaw lets a stolen password work without the expected second factor, MFA stops protecting against password reuse and phishing. That is why the deadline is two weeks, not three.

01 / SONICWALL · CONTINUED FIELD GUIDE

Which build fixes what

Line	Affected	Fixed (per SonicWall)	Notes
Gen 8	8.2.2-8015 and older	**8.2.3-8015** (scheduled Nov 6)	Release notes list the SSL-VPN enforcement fix. Platforms: TZ80–TZ680, NSa 2800–6800, NSv. [2]
Gen 7	7.3.3-7015 and older	**7.3.4-7013 or later**; 7.3.4-7015 scheduled Nov 5	The 7013 notes (Oct 14) list no security fixes, and say 7.3.4 for **NSv** was "not yet released." Install the newest 7.3.4 build for your model and confirm it against the PSIRT page.[1][3]
Gen 6	End of support	No fix	Replace, or take SSL-VPN off the internet.[1]

Same advisory, other fixes (Gen 8 release notes)

- Pre-authentication heap overflow in SSL-VPN
- Pre-auth heap and stack overflows in TACACS+
- Session validation vulnerability
- Weak password hashing

SonicWall's notice lists CVSS 8.8 (High) for the advisory but doesn't say which issue that score belongs to, so we don't give a CVSS score for CVE-2026-19868.[1][2]

What defenders should look for

- SSL-VPN logins that used a method other than the one your policy requires.
- VPN sessions with no matching sign-in at your identity provider.
- New source countries or hosting-provider IPs, and logins at odd hours.
- Privileged internal access soon after a VPN session starts.

Gaps in identity-provider logs can be telemetry loss rather than bypass. Confirm with the firewall's own records.

How to investigate

Export firewall authentication and SSL-VPN logs before upgrading, because a firmware reboot can roll local logs over. Match each session to a user, auth method, source IP and time. Review every configured authentication method, including local users and legacy RADIUS or LDAP fallbacks you may have forgotten.

Contain and remediate

1. Restrict SSL-VPN to required users and source ranges while you prepare the upgrade.
2. Disable authentication methods you don't need.
3. Save logs and the configuration file.
4. Install the fixed build on every node, including HA standby units.
5. Reset credentials and end sessions for accounts with suspicious logins.

Verify recovery

Record the running firmware on each unit. With a test account, confirm that each permitted login path enforces the second factor, and that a disabled method is refused. Check that logging to your SIEM has resumed.

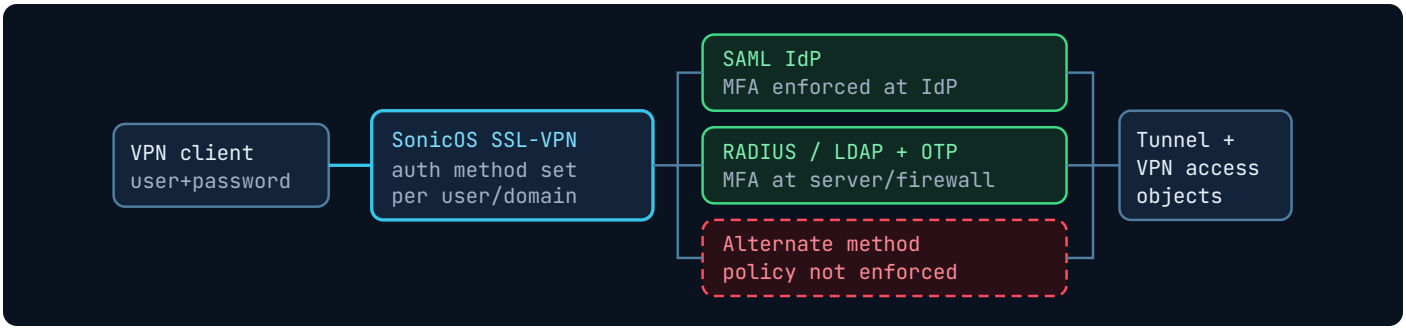
Also from SonicWall this week

On Nov 5 SonicWall said it will not fix two flaws in its end-of-life Global Management System (GMS): CVE-2026-109593, a critical unauthenticated file read, and CVE-2026-109594, an SQL injection. If GMS is still running, isolate it and plan its replacement.[30][31]

01 / SONICWALL · DEEP DIVE TECHNICAL

Where the second factor lives, and how to prove it was enforced

CISA files CVE-2026-19868 under “Use of Single-factor Authentication,” the title of CWE-308. A login path that should require two proofs of identity accepted one. Here is how to model, hunt and close it.



Generic model of SSL-VPN authentication paths, not the vendor’s bug analysis; which method is “alternate” in this CVE is not disclosed. Red dashed box: the bug class, per SonicWall’s release-note wording and CWE-308. Diagram: MAG212 CYBER.[2][6][40]

Threat model: what one factor buys an attacker

An SSL-VPN tunnel puts the client on the internal networks allowed by the user’s VPN access objects. **Hypothetical, not observed in this case:** attackers with a VPN foothold typically enumerate Active Directory, harvest credentials and move toward hypervisors and backups. Scope with your own logs.

Hunting logic (adapt to your SIEM)

The strongest signal is a **VPN session with no matching second-factor event**. For SAML users, that is a firewall login with no identity-provider sign-in for the same user within a few minutes. For RADIUS/OTP users, it is a VPN login with no OTP success on the RADIUS server.

READ-ONLY · SIEM · generic pseudo-query · field names are placeholders

```
-- VPN logins in the last 30 days with no IdP/OTP success for the same user ±5 min
SELECT v.time, v.user, v.src_ip, v.auth_method
FROM   firewall_vpn_logins v
LEFT JOIN idp_mfa_success m
  ON  lower(m.user) = lower(v.user)
  AND m.time BETWEEN v.time - INTERVAL '5' MINUTE AND v.time + INTERVAL '5' MINUTE
WHERE  v.time > now() - INTERVAL '30' DAY AND m.user IS NULL;
```

Illustrates the logic only; it is not a product query. SonicOS log message names and fields differ by version, so map them from your own syslog samples first. False positives: clock skew, UPN vs sAMAccountName, service accounts. Not executed by MAG212.

READ-ONLY · Linux/macOS · nmap · your own public IPs only

```
nmap -Pn -p 443,4433 --script ssl-cert <firewall-public-ip>
```

Shows which ports answer from the internet. 4433 is the usual SonicOS SSL-VPN port; yours may differ. Run from outside, with written authorization. Not executed by MAG212.

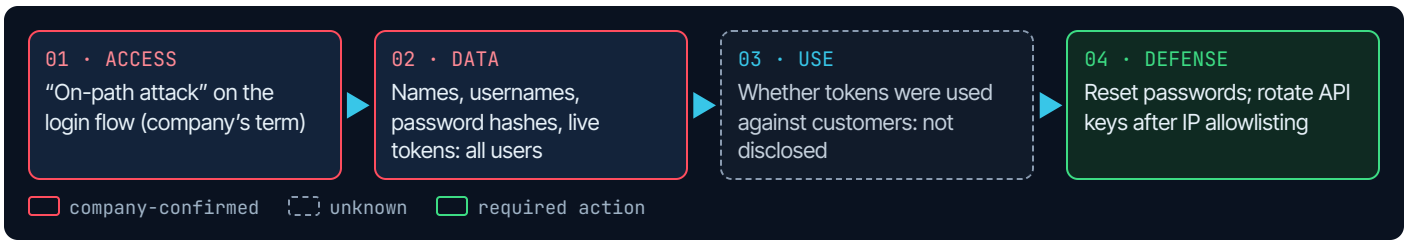
Hardening control	Why it helps here
Remove unused SSL-VPN auth methods and local users	Shrinks the “alternate” paths the bug can use. Pair with least-privilege VPN access objects to limit what a bypassed login reaches.
Restrict SSL-VPN by source (Geo-IP / allow-lists)	Cuts the exposed surface while you patch. SonicOS has Geo-IP and Botnet filters; menu labels vary by version.
Syslog to an external SIEM; management off the WAN	Keeps evidence off the appliance, and limits exposure to the advisory’s pre-auth memory flaws.

02 / DATA BREACH SCOPE WIDENED

Chainalysis: every user's credentials exposed

The blockchain-analytics company first said a subset of customer passwords was affected. Its Nov 6 update says names, usernames, password hashes and live tokens for all users were exposed, and key compliance services are offline.

INCIDENT	UPDATE	OFFLINE	ATTACKER
Began Oct 30	**Nov 6 · all users**	**KYT UI & API, screening, Reactor, Data Solutions**	**Not identified**



Based on Chainalysis's incident page and The Hacker News. Diagram: MAG212 CYBER.[7][8]

What happened

Confirmed (Chainalysis): The company's incident page, first posted for an Oct 30 incident, now says the exposure covers names, usernames, password hashes and live tokens for all users. The KYT interface and API, address screening, the login page, Reactor and Data Solutions are offline or locked. Chainalysis says it has no evidence that investigation or attribution data was touched.[7][8]

Company's description: it attributes the intrusion to an unidentified attacker using "offensive agentic techniques." It has not published technical evidence for that description.[7]

Who is affected

Every Chainalysis user. That includes exchanges, banks, compliance teams and law-enforcement agencies that rely on KYT transaction monitoring and Reactor investigations.

Why it matters

MAG212 analysis: Live tokens can matter more than password hashes, because a valid token may work without the password or MFA. With KYT offline, crypto businesses may also have a gap in automated transaction screening, which is a compliance risk on top of the security one.

What to do now

- Reset Chainalysis passwords for all users. Change the same password anywhere it was reused.
- Rotate API keys once IP allowlisting is configured, as the company directs.
- Find every system that stores a Chainalysis key: scripts, CI secrets, vaults.
- Review API logs for calls from unexpected IPs since Oct 30.
- Document the alternative screening you use while KYT is down, for your compliance records.

Verify recovery

Confirm that old keys are rejected, that integrations work with new keys, and that allowlisting blocks calls from addresses outside your ranges.

Awareness

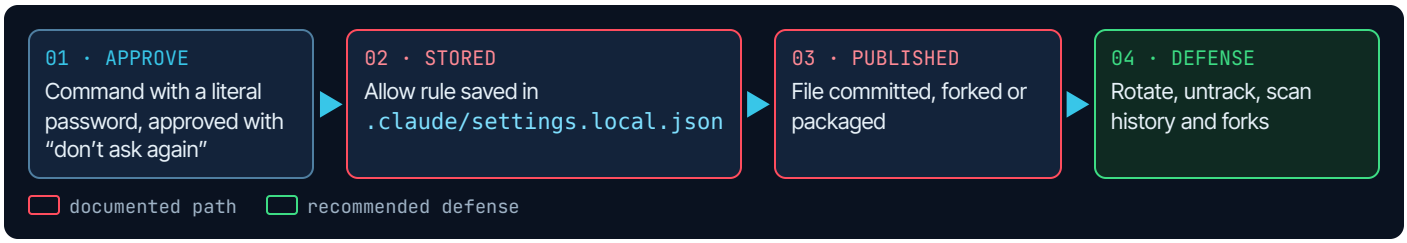
Expect phishing that refers to the breach. Accept reset instructions only through the vendor's own portal or your account manager.

03 / DEVELOPER SECURITY RESEARCH

“Don’t ask again” can write your secrets to disk

When a developer permanently approves a shell command in Claude Code, the full command is saved to a local settings file. Apiiro found over a thousand of those files in public GitHub repositories containing working-looking credentials.

FILES WITH SECRETS	DISTINCT SECRETS	RESEARCH	VENDOR FIX
1,122 of 104,185	1,379	Apiiro · Nov 6	None reported



Exposure path as described in reporting on Apiiro’s research. No misuse of any found credential is documented. Diagram: MAG212 CYBER.[9][11]

What happened

Reported (Apiiro, via The Hacker News, Nov 7): Of 104,185 public copies of `.claude/settings.local.json` in 103,617 repositories, 1,122 held at least one secret: 1,379 distinct secrets, including 379 database passwords, 43 SSH logins, 42 GitHub, GitLab or npm tokens, and 23 AWS keys. Another 734 sat in older, deleted versions, and 211 forks of 74 repositories carried the same secrets. Shared `.claude/settings.json` files had 298 hits out of 76,011.[9]

Apiiro did not test whether the credentials still work. One notified company confirmed its key had been live. We could not load Apiiro’s own post, so these figures come from The Hacker News.[9][10]

Who is affected

Teams using Claude Code whose local settings can end up in a commit, package or archive. Of 16 coding agents Apiiro compared, only Claude Code was confirmed to save the full approved command by default. That doesn’t mean other tools’ folders (`.cursor/` , `.gemini/` , `.specstory/`) are safe, and they are worth scanning too.[9]

How it works

Confirmed (Anthropic docs): “Yes, and don’t ask again” saves an `allow` rule to `settings.local.json` . The first time Claude Code writes that file in a git repository, it adds `**/.claude/settings.local.json` to your **global** git excludes, not the project’s `.gitignore` . A teammate without that global rule, a file created by hand, or a file already committed is not covered.[11]

Scanners miss some

gitleaks caught 564 of the 1,122 files and TruffleHog caught 643; 215 were missed by both. Many secrets are plain passwords inside commands, not keys with a recognizable format.[9]

Vendor response

The Hacker News reports no reply from Anthropic. A related GitHub issue from August 2025 was closed by a bot as “not planned.”[9]

03 / FIELD GUIDE TECHNICAL

Find, scan and prevent: agent settings in Git

What a leaked approval looks like, how to find it in history without printing secrets, and a scanner rule for inline passwords.

ILLUSTRATIVE · not real data · placeholder secret

```
{
  "permissions": {
    "allow": [
      "Bash(npm run test:*)",
      "Bash(psql postgresql://app:<REDACTED-PASSWORD>@db.internal:5432/prod -c:*)"
    ]
  }
}
```

The shape of a `.claude/settings.local.json` allow list, per Anthropic's settings docs. The second rule shows how approving a command that contains a connection string stores the credential with it. Example written by MAG212.[11]

READ-ONLY · Linux/macOS · Bash · Git · authorized full clone

```
# tracked now?
git ls-files -- '.claude/*' '.cursor/*' '.gemini/*' '.specstory/*'
# ever committed, on any branch (commit, date, author)
git log --all --format='%h %ad %an' --date=iso-strict -- '.claude/*'
# ignored locally, and by which rule? (global excludes don't protect teammates)
git check-ignore -v .claude/settings.local.json
```

Lists paths and metadata only. A shallow clone hides history. Syntax checked against Git docs; not executed by MAG212.[32][33]

CHANGE (adds a file) · .gitleaks.toml · gitleaks v8

```
[extend]
useDefault = true                    # keep built-in rules

[[rules]]
id = "inline-cli-password"
description = "Password passed on a command line or env var"
regex = '''(?i)(?:--password[= ]|PGPASSWORD=|MYSQL_PWD=)([^\s'"]{6,})'''
secretGroup = 1

[[rules]]
id = "credential-in-url"
description = "user:password@ in a connection URL"
regex = '''[a-z][a-z0-9+.-]*://[^:/\s@]+:([^@/\s]{4,})@'''
secretGroup = 1
```

A starting point; expect false positives. To scan all history with redacted output (read-only; writes no report unless you ask): `gitleaks detect --source . --log-opts="--all" --redact --config .gitleaks.toml`. Newer releases also offer `gitleaks git`. Not executed by MAG212.[41]

If you find a secret

1. Tell the owner, and never paste the value into tickets.
2. Rotate it at the provider, then review the provider's audit logs back to the first commit.
3. Untrack the file and add `.claude/settings.local.json` to the **project** `.gitignore`.
4. Rewrite history only through the repo owner. Forks keep their copies, so rotation is the real fix.

Prevent it: keep secrets in environment variables or a secrets manager, run the rule pre-commit and in CI, and approve risky commands once, not forever.

04 / REMOTE ACCESS · UPDATE TO NOV 6 EXPLOITATION ATTEMPTS

SSHole: attempts now come from 11 IPs in 8 countries

Yesterday's issue covered the OpenSSH password bypass on musl systems such as Alpine. What's new: probing has spread beyond a single source, and the honeypot root login is now attributed to Previdian's CEO.

CVE	NOV 6 COUNT	NOV 7 COUNT	CISA KEV
CVE-2026-123158	8 attempts · 1 IP (Japan)	17 attempts · 11 IPs · 8 countries	Not listed

What changed

Confirmed (Previdian sensor page, read Nov 7): 17 exploitation attempts seen by 4 sensors, from 11 IP addresses in Switzerland, Denmark, Iran, Japan, the Netherlands, Norway, Singapore and the US. First seen Nov 6, last seen Nov 7. On Nov 6, The Hacker News reported 8 attempts from one IP in Japan.[12][13]

Reported claim: Previdian founder and CEO Ryan Dewhurst told The Hacker News that attackers "used oversized passwords to bypass authentication" on a honeypot and then ran `id`, `uname` and `hostname`. Previdian's public page doesn't describe that login and no raw logs are public. Attempts are not successes.[12][13]

Not CISA KEV: Previdian's page shows "Added to Previdian KEV," the company's own list. CISA had not listed the CVE as of its Nov 6 catalog.[6][12]

Who is affected (Alpine advisory)

- sshd built without PAM, or running with `UsePAM no`.
- `PasswordAuthentication yes` (the default).
- A reachable account whose password field is `*`.
- At least one local account with a `$5$` or `$6$` hash.

Root ships as `root:*` but is reachable only with `PermitRootLogin yes`, or through another account that can become root, for example via `doas`. Official tiny-cloud images 3.18.11–3.24.3 become exposed once any `$6$` hash exists.[14]

How it works

The attacker sends a password of 257–1024 bytes. musl's `crypt()` returns `*` as an error marker for keys over 256 bytes, and that matches the stored `*`. OpenSSH 10.6p2 adds a workaround in sshd and says the root cause lies outside it.[14][15]

Alpine branch	edge	3.24	3.23	3.22	3.21	3.20	3.19	3.18
Fixed openssh	10.6_p2-r0	10.3_p1-r2	10.2_p1-r1	10.0_p1-r11	9.9_p2-r1	9.7_p1-r6	9.6_p1-r3	9.3_p2-r4

Also fixed: 3.17 (9.1_p1-r7) and 3.16 (9.0_p1-r6). Fixed point releases: 3.21.10, 3.22.8, 3.23.8, 3.24.4. Restart sshd after upgrading.[14]

READ-ONLY · Alpine Linux · ash · root

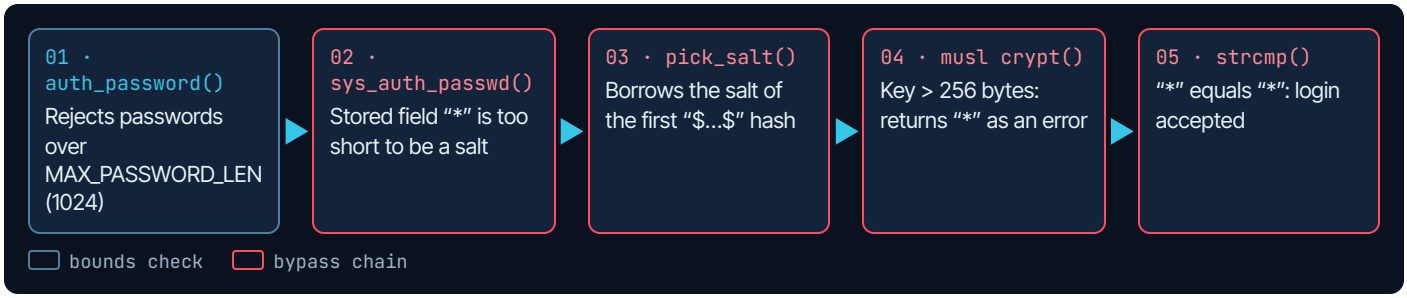
```
apk info -v 2>/dev/null | grep '^openssh'
sshd -T | grep -Ei '^(usepam|passwordauthentication|permitrootlogin) '
```

Shows installed package versions and the effective sshd settings. `sshd -T` needs root to read host keys. It shows configuration, not whether the running daemon was restarted. Syntax checked against sshd(8); not run on an Alpine host.[35]

04 / SSHOLE · DEEP DIVE CODE-LEVEL

Inside the bug: how "*" == "*" became a login

Three behaviors that each look correct combine into a bypass. Here is OpenSSH's non-PAM password path, read alongside Alpine's advisory.



Steps 01–03 come from OpenSSH-portable source (auth-passwd.c, openbsd-compat/xcrypt.c); steps 04–05 from Alpine's advisory. Linking step 03 to the "5/6" condition is MAG212's reading of the code. Diagram: MAG212 CYBER.[14][38][39]

Why 257 to 1024 bytes

`auth_password()` refuses any password longer than `MAX_PASSWORD_LEN`, which is defined as 1024. musl's `crypt()` fails on keys longer than 256 bytes. Anything in between makes `crypt()` fail.[14][38]

Why the target must store *

`sys_auth_passwd()` uses the stored field as the salt only if it has at least two characters. A lone `*` does not, so `xcrypt()` calls `pick_salt()`. That function walks the password database and takes the salt from the first entry that starts with `$`. The result is checked with `strcmp()`, and musl's error string `*` equals the stored `*`.[38][39]

MAG212 reading: locked fields such as `!` don't equal `*`, so shouldn't match. Alpine names only `*`.

Why a 5/6 account is needed

If no `$…$` hash exists, `pick_salt()` falls back to the legacy DES salt `"xx"`. a different `crypt()` path that, per Alpine's conditions, avoids the `*` error. One user with a password exposes **every** `*` account on the host.[14][39]

What logs can and can't show

sshd logs `Accepted password for <user> from <ip>` on success. Password length is not logged and is hidden from network IDS by encryption. The best signal is a **password** login to an account meant for keys only. Alpine's busybox syslog defaults to `/var/log/messages`.

READ-ONLY · Alpine Linux · ash · root · prints account NAMES only, never hashes

```
# accounts whose password field is exactly "*" (bypass targets)
awk -F: '$2=="*"{print $1}' /etc/shadow
# accounts with SHA-256/512 hashes (these enable the salt borrow)
awk -F: '$2 ~ /^\$[56]\$/{print $1}' /etc/shadow
# successful PASSWORD logins (compare with your key-only policy)
grep 'Accepted password for' /var/log/messages*
ls -la /root/.ssh /home/*/.ssh 2>/dev/null; cat /etc/crontabs/* 2>/dev/null; rc-update show   #
persistence
```

If the first two commands both return names and password authentication is on, the host meets Alpine's exposure conditions. Directory-service users may not appear in `/etc/shadow`. Not executed by MAG212.

CHANGE · Alpine · root · from Alpine's advisory · keep an existing session open

```
apk upgrade -U -a && rc-service sshd restart        # the fix
# or, as a stopgap, turn off password auth (drop-in dir is read by default from 3.19)
mkdir -p /etc/ssh/sshd_config.d
echo 'PasswordAuthentication no' > /etc/ssh/sshd_config.d/00-no-passwords.conf
sshd -t && rc-service sshd restart && sshd -T | grep -i passwordauthentication
```

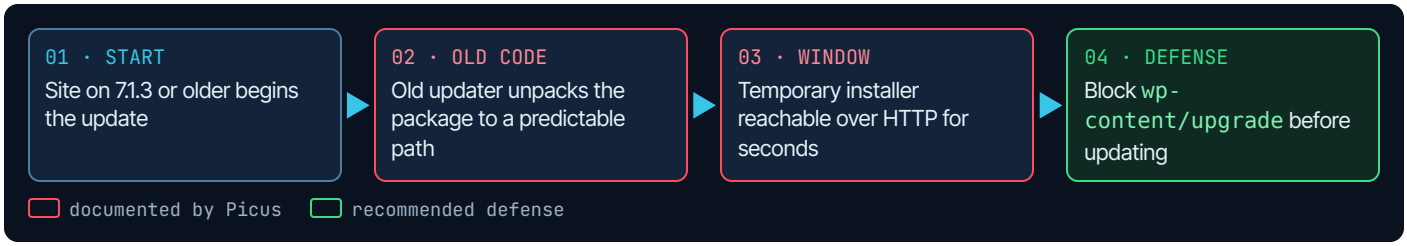
Confirm key login works first. Alpine's advisory also has a `sed` edit for older releases and rollback steps.[14]

05 / WEB PLATFORM · UPDATE TO NOV 5–6 UPGRADE WINDOW

WordPress: guard the first update

The fix for exploited CVE-2026-119977 is installed by the old, vulnerable updater. Researchers explain the brief exposure during that first upgrade and the one rule that closes it.

CVE	KEV	FIXED	WINDOW
CVE-2026-119977	Nov 3	7.1.4 · backports to 4.7	"Only seconds" (Wordfence)



Based on Picus Security's analysis and The Hacker News. Later updates get the new protections. Diagram: MAG212 CYBER.[16][17]

What's new

Confirmed (Picus, Nov 5): During the first upgrade, the old updater does the extraction. The new `update-core.php` still blocks the `wp-config.php` swap, but the random folder name and protective `index.php` only apply to later updates. So the temporary installer sits at a predictable path while the upgrade runs. The flaw dates back to 2.7. Fixes go back to 4.7; 2.7–4.6 get none. [16][18]

Reported (The Hacker News, Nov 6): Wordfence's lab tests found the window lasts "only seconds." Going from 7.1.3 to 7.1.4, WordPress.org's update service offered a partial package, while 7.0.7 to 7.1.4 got only complete packages. WordPress rates the flaw low; Wordfence scores it CVSS 8.1.[17]

Who is affected

Sites still on 7.1.3 or an older unpatched branch release that have not yet run the fixed update. Sites already on 7.1.4 or a patched backport are past this window for this fix.[16][18]

What to look for

Web requests under `/wp-content/upgrade/` around update times, new PHP files there or in the web root, and new admin accounts. One request is a lead, not proof: correlate with server, CDN and WAF logs.

Contain and remediate

Picus advises adding the block in the **root** `.htaccess`, not inside the upgrade folder, because the old updater empties that folder. It also says `wp core update` through WP-CLI is not a safe substitute. Confirm the rule returns 403 before you update.[16]

CHANGE · Apache 2.4 + mod_rewrite · root .htaccess · site admin

```
# Add ABOVE the "# BEGIN WordPress" block. Remove only after every site is updated.
<IfModule mod_rewrite.c>
RewriteEngine On
RewriteRule ^wp-content/upgrade/ - [F,L]
</IfModule>
```

MAG212 example of the approach Picus describes; not tested by us. Nginx, LiteSpeed and managed hosts need their own equivalent, so ask your host. Back up `.htaccess` first. Then check: `curl -sI https://example.com/wp-content/upgrade/` should return **403**. After updating, run `wp core verify-checksums` (read-only).[16][34]

Verify recovery. Confirm the installed version on each site, that the upgrade path returned 403 during the update, and that core checksums match. Check plugins, users and scheduled tasks separately, since checksums cover core files only. Keep the rule if you manage many sites and update in waves.

05 / WORDPRESS · DEEP DIVE HUNT & HARDEN

Block, update, then hunt: commands for every web stack

The upgrade window lasts only seconds, but the original flaw was exploited before the fix existed. Treat the update as the start of your checks, not the end.

1 · Block the staging path (pick your server)

Stack	Rule (CHANGE · site admin · back up config first)	Notes
Apache 2.4	`RewriteRule ^wp-content/upgrade/ - [F,L]` in the root `.htaccess`, above `# BEGIN WordPress`	Needs mod_rewrite. Full block on the previous page.
LiteSpeed	Same `.htaccess` rule	LiteSpeed reads Apache rewrite rules. Purge its cache, then test.
nginx	`location ^~ /wp-content/upgrade/ { deny all; }` in the server block	`^~` stops regex PHP locations from matching first. Run `nginx -t`, then reload. [44]
Managed host	Ask the host	Many run updates themselves; confirm how.

READ-ONLY · any OS · curl · test from OUTSIDE the server

```
curl -s -o /dev/null -w '%{http_code}\n' https://<site>/wp-content/upgrade/
curl -s -o /dev/null -w '%{http_code}\n' https://<site>/wp-content/upgrade/x.php
```

Both should print **403**. A 404 on the second can mean a PHP handler matched first, so check your server's rule order. A CDN cache can hide what the origin does, so test the origin too.

2 · Hunt after updating

READ-ONLY · Linux · Bash · WP-CLI 2.x · site owner shell account

```
# requests to the staging path (log paths vary by distro and host)
zgrep -hE '"(GET|POST) /wp-content/upgrade/' /var/log/{apache2,nginx}/access.log* 2>/dev/null
# PHP files changed since the 7.1.4 release (expect legit updates; review the rest)
find /path/to/wordpress -name '*.php' -newermt '2026-10-28' \
  -not -path '*/wp-content/cache/*' -printf '%TY-%Tm-%Td %TH:%TM %p\n' | sort
# integrity of core and wordpress.org plugins
wp core verify-checksums --path=/path/to/wordpress
wp plugin verify-checksums --all --path=/path/to/wordpress
# administrators and when they were created
wp user list --role=administrator --fields=ID,user_login,user_email,user_registered \
  --path=/path/to/wordpress
```

Uses GNU `find` (`-newermt`, `-printf`); BusyBox and macOS versions differ. Checksums cover only core and wordpress.org plugins, so review premium plugins, themes and `wp-config.php` by hand. A request to the staging path is a lead, not proof of compromise. Syntax checked against WP-CLI docs; not executed by MAG212.[34][43]

3 · If you find something

1. Snapshot the site and database before changing anything.
2. Put the site in maintenance mode or behind a WAF block.
3. Replace core from a clean package. Copy unknown PHP files for analysis, then remove them.
4. Rotate database credentials, the salts in `wp-config.php`, admin passwords and any API keys stored in plugins.
5. Review scheduled tasks (`wp cron event list`) and must-use plugins in `wp-content/mu-plugins`.

Why the window exists

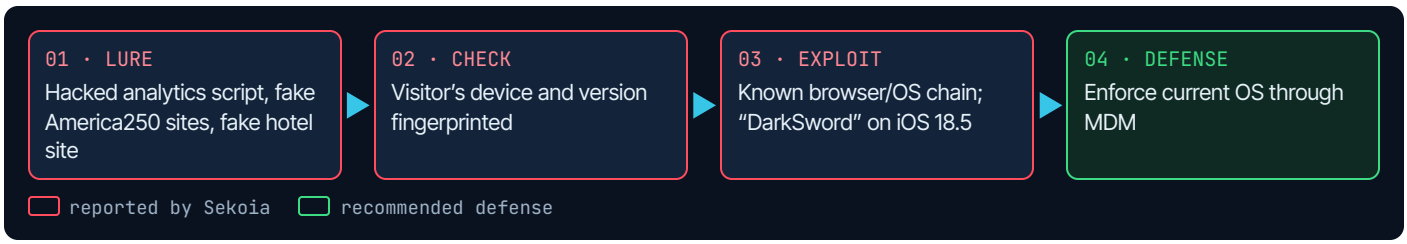
According to Picus, the first upgrade runs the old extraction code. The new random directory name and protective `index.php` only take effect from the **next** update, though the new `update-core.php` still blocks the config swap during this run.[16]

06 / MOBILE THREATS STATE-BACKED

APT29 hits unpatched phones through hacked websites

Sekoia says Russia's APT29 used compromised and fake websites to run known exploit chains against iPhones and Android phones. Some needed no click. Fully updated devices were not affected.

RESEARCHER	ATTRIBUTION	TARGETS	EXPLOITS
Sekoia · Nov 4	APT29 / SVR (Sekoia)	iOS 16, iOS 18.5, old Android Chrome	Already patched (n-day)



Sequence per Sekoia's report and The Record's coverage. Step 02 is MAG212's summary of how watering holes typically select targets; exact selection logic varies by chain. Diagram: MAG212 CYBER.[19][20]

What happened

Researcher claims (Sekoia): The campaign used watering holes, which are legitimate or look-alike sites that visitors already trust. They included a compromised Plerdy analytics script used by thousands of mostly Ukrainian sites (late August to early September), fake America250 sites, and a fake site for the Raffles London at The OWO hotel.[19]

On iOS 16 the chain stole browser cookies. On iOS 18.5 the "DarkSword" toolkit extracted messages, email, passwords, photos, location and WhatsApp and Telegram data. Older Chrome on Android was also targeted. Sekoia names victims including a Ukrainian gas producer, a major US chemical trade association and a European political party.[19][20]

What is not known

Coverage names no CVEs and gives no victim count. Attribution is Sekoia's assessment.[20]

Who is affected

Anyone running out-of-date mobile software, especially staff at energy, chemical, policy and Ukraine-linked organizations, and executives who travel.

What defenders should do

- Use MDM to block corporate access from outdated iOS and Android versions.
- Consider Lockdown Mode on iOS for high-risk staff.
- Inventory third-party scripts on your own websites and use Subresource Integrity or a content security policy[42], so you don't become someone else's watering hole.
- If a device is suspected, preserve it, take it off the network, and get mobile forensics help. Don't just factory-reset it.

For leaders

A phone that is "only a few versions behind" can be compromised just by browsing. Make updates mandatory, not optional.

07 / DATA EXPOSURE BRIEFS

Three disclosures worth your attention

DigiCert: a migration left a business system open for 20 months

Disclosed Oct 20 · new coverage Nov 6 | Certificates not affected | No count published

Confirmed (DigiCert's Mozilla incident report): A Feb 4, 2025 migration moved a business system out of a VPN-only segment and onto the internet. A registration feature "meant for other use cases" let outsiders create accounts that skipped MFA and got read-only access, which still reached customer archives.[21]

Staff noticed outside accounts on June 18, 2026 but concluded they had no data access. Data was accessed from **June 27 to July 2**, when an authorization fix closed the gap. DigiCert first suspected data access Oct 12, confirmed it Oct 19, and turned off self-registration Oct 24.[21]

Data: mostly business contact details. For "a small minority" of accounts, documents such as a driver's license, passport or utility bill. DigiCert says customer login credentials and issued certificates "remain secure, valid, and fully trusted." This is separate from DigiCert's spring 2026 code-signing incident.[21][22]

MAG212 lesson: make external reachability and authorization checks part of the acceptance criteria for every network migration. A read-only role can still leak confidential records.

Norad: grants portal breach may affect 20,614 users

Nov 5 | Attacker unknown

Reported (Help Net Security): Norway's development agency found on Oct 30 that attackers had logged into its grants portal with 27 compromised accounts and stolen applications from three non-Norwegian organizations. All 20,614 registered users, across 12,511 organizations, may be affected, including applicants in conflict zones and authoritarian states. Norway's security authority, NSM, says the attack shares traits with other recent incidents.[23]

Queens Public Library: ransomware hits 66 branches

Ransomware | No group named

Reported (The Record, Nov 5): The attack took down on-site computers, self check-out, Wi-Fi, digital media and the mobile app. All branches serving about 2.3 million residents stayed open. For school and library IT teams: keep manual check-out and offline procedures documented and practised.[24]

08 / POLICY AND AI BRIEFS

Faster attackers, faster responses

Japan adopts an emergency cybersecurity package

Nov 6 · Ministerial Meeting on Cybersecurity | Government decision

Confirmed (government summary): Japan's Ministerial Meeting on Cybersecurity, chaired by Prime Minister Takaichi, adopted the package on Nov 6. At the group's Oct 26 meeting, she had asked for one within about a week. It names unpatched flaws, misconfiguration, weak security during development, and gaps at contractors as weaknesses that AI is making faster to exploit.[25]

Selected measures:

- An IPA "Top Gun" team, from November, to expand penetration testing with private firms.
- Teams to help municipalities run AI-assisted vulnerability checks.
- A police rapid forensic unit (working name) to preserve logs early.
- Backup and recovery support added to the Cybersecurity Support Squad service for small businesses.
- Expert response teams, scaled up to multi-ministry teams for major incidents.
- A 24/365 monitoring pilot run by IPA and NICT.

The summary gives no budget figures. **MAG212 takeaway:** run a timed exercise from first alert to approved containment, and know which outside responders you can call.[25]

OpenAI restricts its cyber model to vetted organizations

Nov 5 · system card | Rated "Critical" for cyber by OpenAI

Confirmed (OpenAI): GPT-6 Cyber, a cyber-specialized variant of GPT-6 Astra, is available only through the Daybreak Red program. Individuals need an invitation, identity and liveness checks, a legal attestation and a physical FIDO2 key. Organizations need SSO, MFA, managed devices and least-privilege access; API access requires IP allowlisting by default. OpenAI reports gains over Astra on its exploitation benchmarks. Benchmark results are not evidence of real-world attacks.[26]

$129 million AI deepfake fraud charged in New York

Nov 5 · DOJ SDNY | Allegations, not convictions

Confirmed (DOJ): Prosecutors charged three men with wire fraud, money laundering and aggravated identity theft. They allegedly used AI to fake the voices and images of real CEOs and lawyers from 2024 to 2026, and laundered about $129 million through crypto. Victims named include hospitals in Missouri (about $5M) and California ($2.9M), a Rhode Island bank ($2.6M) and a UK tech company ($11.5M). Two defendants were arrested in Spain and one is held in the UK.[27] See the awareness lesson on page 17.

DEFENDER'S ACTION DESK

Today's patch and check list

#	Item	Status	Action
1	SonicWall SonicOS CVE-2026-19868	Exploited · KEV	Gen 8 → 8.2.3-8015; Gen 7 → newest 7.3.4 build. Save logs first, cover HA standby units.[1][6]
2	Chainalysis users	Breach	Reset passwords, rotate API keys after allowlisting, review API logs since Oct 30.[7]
3	OpenSSH on Alpine/musl	Attempts seen	Install the branch's fixed `openssh`, restart sshd, or set `PasswordAuthentication no`.[14]
4	WordPress CVE-2026-119977	KEV	Block `wp-content/upgrade`, update, confirm 403, verify checksums.[16]
5	Agent settings files	Research	Find tracked `.claude/` and similar folders; rotate any secrets found.[9]
6	Mobile fleet	n-day campaign	Enforce current iOS/Android via MDM.[19]
7	Microsoft Paint CVE-2026-83844	Not exploited	CVSS 8.1 RCE fixed only via the Microsoft Store (11.2609.401.0 per MSRC), so Windows Update compliance won't show it.[28][29]
8	SonicWall GMS (end of life)	No fix	CVE-2026-109593/-109594 won't be fixed. Isolate GMS and plan replacement.[30][31]

READ-ONLY · Windows · PowerShell 5.1+ · administrator (for -AllUsers)

```
Get-AppxPackage -AllUsers -Name Microsoft.Paint |
  Select-Object Name, Version, PackageUserInformation
```

Lists the Paint version for each user profile, since Store apps update per user. Compare with the fixed build in MSRC's advisory; NVD lists a different affected-version cutoff, so treat MSRC as authoritative. Syntax checked against Microsoft Learn; not executed by MAG212.[28][37]

CISA KEV additions, last ten days

Added	CVE	Product	Federal due date
Nov 6	CVE-2026-19868	SonicWall SonicOS SSLVPN	Nov 20
Nov 4	CVE-2024-27834	Apple, multiple products	Nov 18
Nov 3	CVE-2026-119977	WordPress Core	Nov 6 (passed)
Oct 30	CVE-2026-118527, CVE-2026-111357	Ivanti Connect Secure	Per catalog
Oct 29	CVE-2026-97229 · CVE-2026-76418	GitLab · Cisco ASA/FTD	Per catalog

From CISA's KEV data, catalog version 2026.11.06. No additions on Nov 5; none on Nov 7 as of that version. Re-check the catalog before you close tickets.[6]

First hour: establish scope

For each item, record the asset, owner, exact running version, how it's exposed and when you checked. MSPs: keep this per tenant. Schools: test management interfaces from staff, student and guest networks with authorized accounts.

Same shift: protect evidence

Export firewall, VPN, identity and endpoint logs before reboots or upgrades. Note time offsets and retention gaps.

Close the ticket: verify independently

Require the running version, an exposure check from the right network, a configuration comparison and a service test. A patch closes the door; it doesn't tell you who already came in.

Escalate when

You see an unexpected VPN login method, a successful password login to a key-only SSH account, or API calls with an old key. Name one incident lead and keep observations separate from hypotheses.

TWO-MINUTE LESSON · FOR STAFF AND BUSINESS LEADERS

The CEO on the video call may not be the CEO

A call comes in. The voice is your CEO's, maybe with a lawyer on the line too. There's a confidential deal and the wire has to go out today. Prosecutors say this pattern cost hospitals, a bank and companies about $129 million.

What is going on

AI can now copy a voice from a few public clips and put a familiar face on a video call. According to the SDNY charges, the scheme impersonated real executives and attorneys at an international law firm to get urgent payments approved.[27]

Do this every time

- Verify any new payment or change of bank details through a number you already have, not one given on the call or in the email.
- Use a two-person rule for transfers above a set amount, with no exceptions for "confidential" deals.
- Agree a code word or call-back routine with executives for urgent requests.
- Slow down when you hear urgency, secrecy or authority together.

If you already sent money

Call your bank's fraud line immediately and ask for a recall, tell finance and IT, keep every message and call record, and report to the FBI's IC3 (in the US) or your national reporting service.

For leaders

Put payment verification in policy and back the employee who delays a wire to check it. The same applies to breach phishing this week: when Chainalysis or DigiCert customers get "reset now" messages, they should use the vendor's portal, not the link.

Watch list. SonicWall CVE details and a possible 7.3.4-7015 confirmation; whether CISA adds SSHole to KEV; Chainalysis service restoration; Microsoft's November Patch Tuesday on Nov 10.

MAG212 CYBER in your inbox, free

Daily intelligence, new magazine editions, threat alerts and practical cheat sheets for IT teams, MSPs and business owners. Free, and you can unsubscribe anytime.

Subscribe free → cyber.mag212.com/subscribe-free

EDITORIAL TRANSPARENCY

How we checked this issue

Every story was checked against vendor, government or original-researcher sources. Where we couldn't reach a primary page, we say so.

Story	Sources checked	Open questions
SonicWall	SonicWall notice, 8.2.3 and 7.3.4 release notes, Canadian Cyber Centre, CISA KEV data	PSIRT and NVD pages didn't render. CVE-specific CVSS unknown. SAML involvement and credential requirement not confirmed. Gen 7 build that carries the fix is unclear.
Chainalysis	Company incident page, The Hacker News	"Agentic" claim is the company's, without published evidence. No evidence of token misuse published.
Agent secrets	The Hacker News, Anthropic docs	Apiiro's post didn't load; figures via The Hacker News. Credentials not validity-tested.
SSHole	Previdian, Alpine, OpenSSH, The Hacker News	Honeypot root login is a claim without public logs. Not in CISA KEV.
WordPress	Picus, The Hacker News, WordPress.org	No official WordPress.org guidance on the window. .htaccess example untested.
APT29	Sekoia, The Record	No CVEs or victim count published. Attribution is Sekoia's.
Briefs	DigiCert Bugzilla report, SecurityWeek, Help Net Security, The Record, Japan summary, OpenAI, DOJ	No DigiCert count or state filing found. Norad statement and the AP Japan article weren't retrieved.

Changes from the earlier draft of today's issue

- **SonicWall:** removed SAML/MFA and "valid credentials" as stated facts, since no source confirms them. Added the KEV due date (Nov 20), the Gen 7 7013/7015 build question, the NSv note, the advisory's other fixes and the GMS won't-fix.
- **Agent secrets:** Apiiro published Nov 6, not Nov 5. Corrected how the file is excluded: via the user's **global** git excludes, which doesn't cover teammates, hand-made files or files already committed. Added scanner and fork figures.
- **SSHole:** updated to 17 attempts, 11 IPs, 8 countries. Named the source of the root-login claim. Added the exact hash and password-length conditions and the fixed-package table.
- **WordPress:** added Wordfence's "seconds" finding, the root-.htaccess placement, and that 2.7–4.6 get no fix.
- **DigiCert:** added the June 27–July 2 access window and noted it was first disclosed Oct 20. Japan: the package was adopted by the Ministerial Meeting on Cybersecurity.
- **Cut:** the refrigeration fact sheet, with nothing new since our Nov 6 issue.[36] Also cut the SecurityWeek roundup items (Trezor, LLMjacking, SAP), which had no new primary evidence.
- **Added:** Chainalysis, APT29 mobile, Norad, Queens Library, the DOJ deepfake case, Microsoft Paint.
- **Technical edition:** added three deep-dive pages (SonicWall MFA-enforcement hunting, the SSHole code path from OpenSSH source, WordPress block/hunt commands per web server) and a scanner rule for agent settings files. Code-level statements cite OpenSSH-portable source; where we connect two facts ourselves, it is labelled "MAG212 reading."

Visuals and commands. All diagrams are MAG212 CYBER explanatory graphics, and the cover is a conceptual illustration. The draft's stock photos and recreated interface panels were removed. This issue has no screenshots. Commands were checked against official documentation but not executed on affected systems.

EDITORIAL REGISTER

Sources

01 SonicWall · SonicOS 7.3.4 and 8.2.3 security advisory notice (updated Nov 6)
02 SonicWall · SonicOS 8.2.3-8015 release notes
03 SonicWall · SonicOS 7.3.4-7013 release notes (Oct 14)
04 SonicWall PSIRT · SNWLID-2026-0014 (page did not render for us)
05 Canadian Centre for Cyber Security · AV26-1133 (Nov 6)
06 CISA · KEV catalog data, version 2026.11.06 (official GitHub mirror)
07 Chainalysis · Security incident update (Nov 6)
08 The Hacker News · Chainalysis breach exposes all users (Nov 6)
09 The Hacker News · Claude Code 'don't ask again' file leaks secrets (Nov 7)
10 Apiiro · Coding agents leaking secrets (Nov 6; did not load for us)
11 Anthropic · Claude Code settings documentation
12 Previdian · CVE-2026-123158 sensor page (read Nov 7)
13 The Hacker News · Hackers exploited OpenSSH 'SSHole' flaw (Nov 6)
14 Alpine Linux · OpenSSH password authentication bypass (Nov 5)
15 OpenSSH · Release notes, 10.6p2 (Nov 5)
16 Picus Security · When updating WordPress becomes the vulnerability (Nov 5)
17 The Hacker News · Installing the fix for exploited WordPress flaw (Nov 6)
18 WordPress.org · WordPress 7.1.4 security release (Oct 28)
19 Sekoia · APT29 watering holes target mobile devices (Nov 4)
20 The Record · Russian hackers target smartphones (Nov 5)
21 Mozilla Bugzilla 2084460 · DigiCert incident report (from Oct 20)
22 SecurityWeek · DigiCert breach impacts business customer info (Nov 6)
23 Help Net Security · Norad grants portal breach (Nov 5)
24 The Record · Queens library ransomware (Nov 5)
25 Government of Japan · Cybersecurity emergency package summary, Nov 6 (Japanese; MHLW copy)
26 OpenAI · GPT-6 Cyber system card (Nov 5)
27 US DOJ, SDNY · Three charged in AI impersonation scheme (Nov 5)
28 Microsoft MSRC · CVE-2026-83844 Paint
29 The Hacker News · Microsoft Paint RCE fix via Store (Nov 6)
30 SecurityWeek · Cisco, WatchGuard patch; SonicWall won't fix GMS (Nov 5)
31 SonicWall PSIRT · SNWLID-2026-0019 (GMS)
32 Git documentation · git-ls-files
33 Git documentation · git-log
34 WP-CLI · wp core verify-checksums
35 OpenBSD manual · sshd(8)
36 CISA/FBI/HHS/USDA/DOT · Refrigeration fact sheet (Nov 5) — no update, not repeated
37 Microsoft Learn · Get-AppxPackage
38 OpenSSH portable · auth-passwd.c (sys_auth_passwd, MAX_PASSWORD_LEN)
39 OpenSSH portable · openbsd-compat/xcrypt.c (pick_salt)
40 MITRE · CWE-308 Use of Single-factor Authentication
41 Gitleaks · README and configuration reference
42 MDN · Subresource Integrity
43 WP-CLI · wp user list
44 nginx · location directive

MAG212 CYBER · Daily Cyber Intelligence · November 7, 2026. Written and edited by El Mostafa Ouchen. Research cutoff 06:55 PST (America/Los_Angeles). Summaries and analysis are original; quotations are attributed. Free subscription: cyber.mag212.com/subscribe-free.