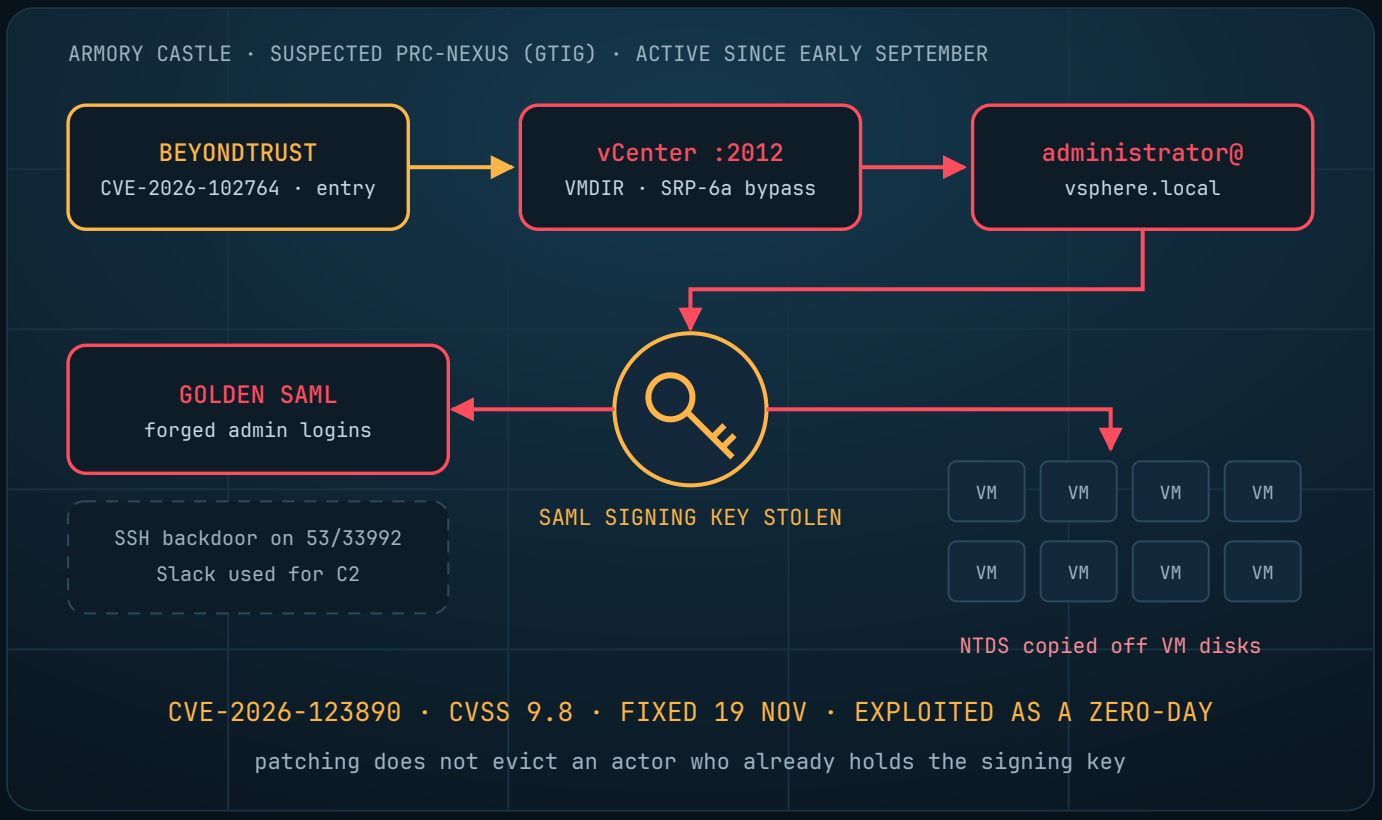
MAG212
CYBER

DAILY

Friday, 20 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 6:00 AM PT



VMWARE vCENTER · CVE-2026-123890

The keys to vSphere

For about ten weeks a suspected Chinese espionage group used an unknown vCenter flaw to become administrator, steal the signing key and forge its own logins. Broadcom shipped the fix on 19 November. Also today: Cisco Expressway is breached in the wild, and SonicWall stops patching Gen 6.

03 vCenter zero-day: the attack chain
05 Cisco Expressway: four devices breached
06 SonicWall Gen 6: no more patches
07 EU Commission: an “AI generated” campaign
08 SBC Medical: at least 1.6M people
09 Ruby2Shell and PHP releases

8.0 U3m
vCenter fix · also 9.0.2.0200 / 9.1.1.0200

ZERO-DAY
exploited since early Sept (GTIG)

X15.5.20
Expressway fix · 4 devices breached (F6)

GEN 6
SonicWall: no patches, any severity

What matters today

Developments published or updated 18–20 November. The Cisco flaw was patched in October; it is included because exploitation was reported on 19 November.

Virtualization under attack

Broadcom fixed a vCenter authentication bypass on 19 November. Google says ARMORY CASTLE had been exploiting it since early September to forge admin logins and copy Active Directory secrets. [1][3]

Old patch, new victims

Cisco fixed a hard-coded credential in clustered Expressway on 21 October. F6 now reports four devices breached at one Russian organisation. Cisco still says it is unaware of malicious use. [8][9]

The end of a firewall line

SonicWall will not patch Gen 6 at any severity. It expects internet-facing units to be "actively targeted" and says hardening does not make them secure. [11][12]

AI in the attack, data in the open

The European Commission confirmed an "AI generated cyber campaign". SBC Medical told the SEC that records of at least 1.6 million people were exposed. [15][17][20][21]

THE THREE PRIORITY ACTIONS

1. **Patch vCenter to 8.0 U3m, 9.0.2.0200 or 9.1.1.0200, then hunt.**
   Block TCP 2012 from everything except other vCenter/PSC nodes. Look for `sps-*@vsphere.local` accounts and the GTIG file paths; if found, rotate the STS signing certificate. [1][3][6]
2. **Upgrade clustered Cisco Expressway to X15.5.20; migrate off X14.**
   Block TCP 4372 between anything but cluster peers. Search logs for `wombat@127.0.0.1`. [8][10]
3. **List every SonicWall Gen 6 and plan its replacement.**
   Until then: no WAN management, SSL VPN off or restricted, MFA on, passwords reset. [11]

EXPLOITATION STATUS AT A GLANCE

ISSUE	STATUS	FIX
vCenter CVE-2026-123890	EXPLOITED · ZERO-DAY	8.0 U3m / 9.x .0200
Expressway CVE-2026-76466	EXPLOITED (F6)	X15.5.20
SonicWall Gen 6	NO PATCHES	replace
Ruby2Shell / PHP	PATCHED · NO ATTACKS	4.0.10 · 8.5.13

CONTENTS

03 vCenter zero-day: the attack chain
04 vCenter: patch, hunt, evict
05 Cisco Expressway exploited
06 SonicWall Gen 6 retired
07 European Commission AI attack
08 SBC Medical breach
09 Ruby2Shell and PHP
10 Briefs
11 Defender's Action Desk
12 Awareness: devices nobody patches
13 Sources

FIXED 19 NOV · VMSA-2026-0009 | CVSS 9.8 | EXPLOITED AS ZERO-DAY (GTIG)

KEV: NOT LISTED (REPORTED)

vCenter zero-day: from directory port to domain secrets

KEY FACT **What happened.** On 19 November Broadcom fixed CVE-2026-123890, an authentication bypass in vCenter's VMware Directory Service reached over DCE/RPC on TCP 2012. An unauthenticated attacker becomes administrator@vsphere.local. Google's GTIG and Mandiant say the flaw was exploited as a zero-day from early September and attribute the activity to "the suspected PRC-nexus espionage actor ARMORY CASTLE (formerly tracked as UNC5221)". [1][3]

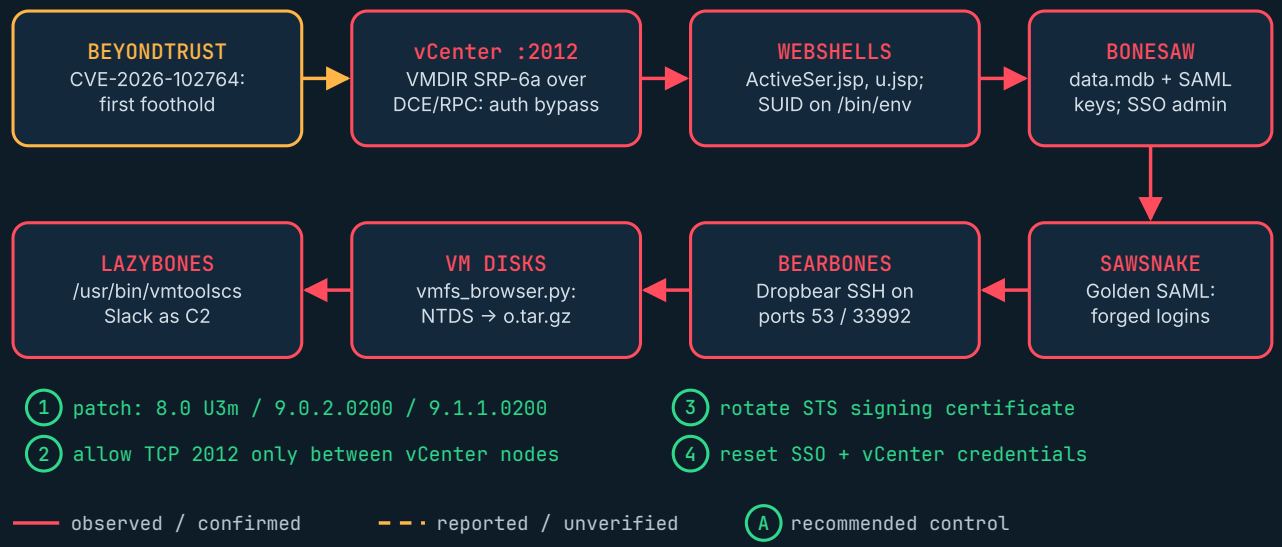


Figure 1 · Intrusion chain per GTIG/Mandiant [3]. Amber = entry through a separate product; red = observed by Mandiant. Diagram: MAG212 CYBER.

HOW THE ATTACK WORKS

The bug sits in the SRP-6a password exchange of the directory service. Once in as SSO administrator, the actor dropped JSP webshells, set SUID on `/bin/env`, and ran BONESAW to copy the directory database (`data.mdb`) and SAML signing keys and to create an SSO admin. SAWSNAKE then forged "Golden SAML" logins. [3]

To stay in, it added a rogue `sps-*@vsphere.local` account, toggled SSH through the appliance REST API, and installed two backdoors. It used `vmfs_browser.py` to read Windows domain controllers' disks directly and pull NTDS. [3]

WHAT IT TAKES

- Network reach to TCP 2012 on vCenter. In Mandiant's case the actor got that reach through a BeyondTrust flaw (CVE-2026-102764). [3]
- No credentials and no user action. Broadcom lists no workaround; the fix is not available as a Quick Patch. [1] [2]
- vCenter 7.0 has no public fixed build: Broadcom says to contact support. [1]

WHO AND WHY

GTIG calls the actor espionage-focused; it is also tracked as Warp Panda. Victim names and counts are not public. Broadcom's advisory does not itself flag exploitation, and the CVE was not in CISA KEV as of 20 November according to the outlets we cite (we could not reach cisa.gov). [1][3][4][5]

vCenter: patch, hunt, evict

VMSA-2026-0009 also fixes SDDC Manager (CVE-2026-123891/2/3) and VMware Tools (CVE-2026-123894).

PRODUCT	FIXED VERSION	NOTE
vCenter Server 9.1	9.1.1.0200	no workaround
vCenter Server 9.0	9.0.2.0200	no workaround
vCenter Server 8.0	8.0 U3m	not a Quick Patch
VMware Cloud Foundation 5.2	5.2.5	updates bundled vCenter
vCenter Server 7.0	none public	contact Broadcom support

Table 1 · From Broadcom's VMSA-2026-0009.1 and its FAQ [1, 2]. Check the advisory for your exact build before you upgrade.

PowerCLI · vCenter admin · READ-ONLY · NOT TESTED BY MAG212

VERSION + ROGUE ACCOUNT

```
Connect-VIServer vcenter.example.com
$global:DefaultVIServer.Version
$global:DefaultVIServer.Build
Get-VIAccount |
  Where-Object { $_.Name -like 'sps-*' }
```

From Ostorlab's write-up, not a Broadcom procedure. Compare the build with the VMSA. Any `sps-*` account you did not create matches GTIG's rogue-account pattern. Not run by MAG212. [6][3]

vCenter appliance · bash · root · READ-ONLY · NOT TESTED BY MAG212

HOST INDICATORS

```
ls -la /tmp/123 /tmp/sss /tmp/dbr \
  /usr/bin/vmtoolscs 2>/dev/null
ls -l /bin/env     # SUID 's' bit?
ss -ltnp | grep -E ':(53|33992) '
# from a user LAN host:
nc -vz vcenter.example.com 2012
```

MAG212 triage suggestion built from GTIG's file and port indicators and Ostorlab's reachability test. The last line should FAIL from ordinary networks. A hit means incident response, not cleanup. [3][6]

INDICATORS (GTIG)

FILES	ActiveSer.jsp · u.jsp · /tmp/123 · /tmp/sss · /tmp/dbr · /usr/bin/vmtoolscs · o.tar.gz
SSH	banner SSH-2.0-pulsesecure_23345 · ports 53, 33992
ACCOUNT	sps–<random>@vsphere.local
IPs	11 “suspected obfuscation network” IPs, e.g. 103.147.251[.]5, 103.190.38[.]3 — full list and YARA rules in [3]

No file hashes are public; GTIG keeps full IoCs in a registered collection. [3]

CONTAIN, FIX, VERIFY

1. Restrict TCP 443, 2012, 22 and 5480 to admin and peer networks (Mandiant vcsa-hardening-tool).
2. Patch every vCenter, including lab and DR instances.
3. If any indicator hits: rotate the STS signing certificate, reset SSO and vCenter credentials, and treat AD as exposed.
4. Verify: new build number; TCP 2012 unreachable from user networks.
5. Check BeyondTrust appliances for the entry bug.

EXPLOITED (F6, VIA THN) | CVSS 9.8 · CWE-798 | PUBLIC POC SINCE 5 NOV | CISCO: "NOT AWARE OF MALICIOUS USE"

Cisco Expressway: a static password, four breached devices

KEY FACT **What happened.** Cisco fixed CVE-2026-76466 on 21 October: clustered Expressway-C and Expressway-E accept a hard-coded credential that gives an unauthenticated attacker root. On 19 November Russian security firm F6 reported that attackers used it against one Russian organisation and compromised four devices. We could not load F6's own report; details come from The Hacker News and Ostorlab. [8][9][10]

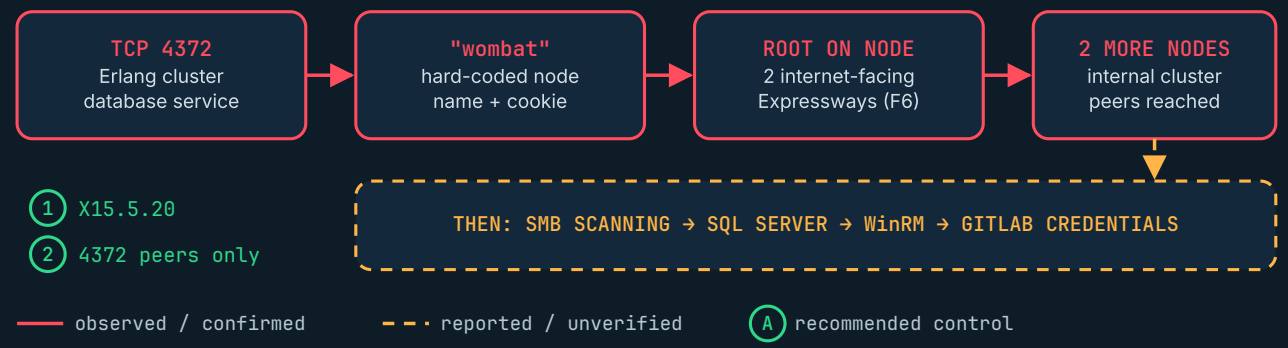


Figure 2 · Exploitation path. Red = reported by F6 and Cisco [8, 9]; amber dashed = post-compromise activity as reported. Mechanism per Ostorlab [10]. Diagram: MAG212 CYBER.

WHO IS AFFECTED

- Expressway-C and -E, virtual and appliance, **only when configured in a cluster**, on X15.5.3 and earlier or X14 and earlier. [8]
- Fixed in X15.5.20. X14 and earlier must migrate to a fixed release. Cisco lists no workaround. [8]
- Cisco blames persistent cookies and weak client-certificate checks when TLS Verify Mode is on for clustering. [8]

WHAT THE ATTACKERS DID

Per THN's account of F6: entry through two internet-facing devices, then two internal cluster nodes. Python scripts, possibly AI-assisted per THN, scanned for SMB; the intruders then moved to SQL Server and WinRM and went after GitLab credentials. No attribution. [9]

INDICATORS (F6, SECOND-HAND)

IPs	66.179.31[.]32 · 18.130.47[.]116
LOG	wombat@127.0.0.1 in erlang.log
FILES	/mnt/harddisk/i<4 digits>[letter]/*.py

Expressway · root shell | root | READ-ONLY | NOT TESTED BY MAG212

HUNT

```
grep -R "wombat@127.0.0.1" \
  /var/log/ 2>/dev/null
find /mnt/harddisk -maxdepth 3 -type f \
  -name '*.py' 2>/dev/null \
  | grep -E '/i[0-9]{4}[A-Za-z]?/'
nc -vz expressway.example.com 4372
```

From Ostorlab, not Cisco: Cisco publishes no compromise checks. Any hit means incident response. The last line, run from a non-peer network, should fail. Not run by MAG212. [10]

WHY IT MATTERS

- A month passed between patch and reported attacks, and a public PoC appeared in between. [9] [10]
- Expressway sits at the edge for video and voice; a root shell there is a route inside. [9]
- Cluster ports are rarely filtered internally. Allow 4371/4372 only between peers (our reading of [10]).

NOTICE 18 NOV | NO PATCHES · ANY SEVERITY | NO NEW CVE NAMED | FIX = REPLACE (GEN 8)

SonicWall Gen 6: the patches have stopped

KEY FACT **What happened.** SonicWall's 18 November notice says it no longer releases firmware or security patches for Gen 6 and 6.5 firewalls, including NSv virtual units, "regardless of severity", with no exception for critical flaws. It expects internet-facing Gen 6 firewalls "to be actively targeted". [11][12]

END OF SUPPORT	GEN 6 / 6.5 MODELS
1 Oct 2026	TZ350/W, TZ500/W, SOHO 250/W; NSA 4600/5600/6600; NSa 4650/5650/6650
1 Aug 2026	TZ400/W, TZ600, TZ600P, NSA 3600; NSa 3650
1 May 2026	NSa 2650
16 Apr 2026	SOHO, SOHO W, TZ300P, NSa 9250/9450/9650; NSv 10–1600
20 Feb 2026	SuperMassive 9200/9400/9600/9800; NSsp 12800, 12400
23 Jan 2025	TZ300, TZ300W
8 Mar 2024	NSA 2600

Table 2 · End-of-support dates as listed in SonicWall's notice [11]. Every model listed is now past end of support.

WHY NOW

SonicWall points to CVE-2024-40766 (CVSS 9.3), an access-control flaw in Gen 5, Gen 6 and early Gen 7 that was exploited in the wild. A unit still on Gen 6 would not get a fix for a bug like that today. It also says attackers use "automation and AI" to find unsupported edge devices faster. [11][12]

THE PATTERN

- Early November: SonicWall said two GMS 9.5.2 flaws (CVE-2026-109593, 9.1; -109594, 6.8) will not be fixed; move to NSM. [14]
- THN reports CVE-2026-102255 (CVSS 10, patched in October) under exploitation. [14]
- Gen 7 and Gen 8 got fixes in SNWLID-2026-0014 (7.3.4-7013, 8.2.3-8015). [13]

UNTIL THE BOX IS GONE (SONICWALL)

1. Disable WAN management: HTTPS, SSH and SNMP.
2. Disable SSL VPN or restrict it to known source addresses.
3. Enforce MFA on remote-access and admin accounts; reset local passwords.
4. Disable unused services and interfaces; watch logs for odd logins and config changes.
5. Inventory spares and branch units too.

SonicWall's words: these steps reduce exposure but do "not make Gen 6 secure". [11]

MIGRATION

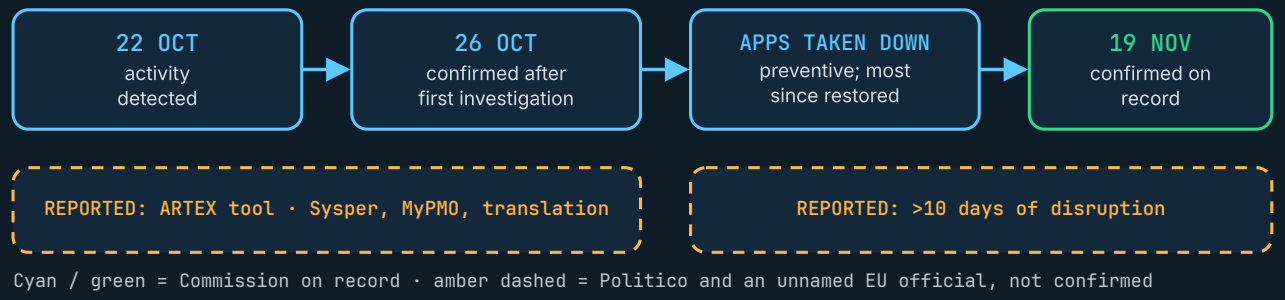
Replace with a Gen 8 on SonicOS 8. Settings can be imported from SonicOS 6.5 with the in-product import or the NSM Migration App. SonicWall also points owners to its Secure Upgrade Plus programme. [11][13]

CONFIRMED 19 NOV | "AI GENERATED CYBER CAMPAIGN" | NO ATTRIBUTION

TOOL NAME: REPORTED ONLY

European Commission: an "AI generated" campaign

KEY FACT **What happened.** At the midday briefing on 19 November, spokesperson Thomas Regnier said "we can confirm that this was an AI generated cyber campaign" involving "a misuse of an AI tool" that is publicly available. The Commission temporarily took down several applications; most are back. [15][16][17]



Cyan / green = Commission on record · amber dashed = Politico and an unnamed EU official, not confirmed

Figure 3 · What is on record versus what is reported [15–18]. Diagram: MAG212 CYBER.

ON RECORD

- No evidence so far of "a data breach affecting Commission staff as a whole". That wording does not rule out access to individual records. [17]
- No ransom demand known; no attribution; "many elements" contained. The Commission is working with CERT-EU and the EDPS. [16][17]
- Regnier did not name the tool, the services hit or the attack method. [17]

REPORTED, NOT CONFIRMED

- Politico, citing an EU official: CERT-EU saw the attackers use ARTEX, an AI penetration-testing framework. SecurityWeek notes this is unconfirmed. [16][17]
- Affected services reportedly included the Sysper HR system, MyPMO medical reimbursement and translation. [16][18]

ABOUT ARTEX (CONTEXT)

- An FBI FLASH reported on 15 November says criminal and state-aligned actors have abused ARTEX since at least August, sometimes reaching privileged access in under three hours. [19]
- GTIG's 16 November tracker lists ARTEX among autonomous multi-agent offensive frameworks. [42]
- Neither the FBI nor GTIG mentions the Commission. Any link rests on the unconfirmed report.

WHAT DEFENDERS CAN TAKE FROM IT

- Assume faster attack timelines: patch internet-facing systems in days, not weeks.
- Alert on bursts of scanning and exploitation from one source across many apps.
- Do not read "AI generated" as "autonomous": no public evidence says how much a human steered it.

THE COMMISSION'S 2026 SO FAR

WHEN	INCIDENT	SOURCE
January	Incident affecting mobile-device management infrastructure	[18]
March–April	Cloud (AWS) breach; CERT-EU traced it to a compromised Trivy supply chain	[18, 43]
22 Oct → 19 Nov	AI-assisted campaign; applications taken down, most restored	[15–17]

Three separate incidents in one year at the EU's executive. The method behind the newest one is still not public.

8-K FILED 18 NOV | AT LEAST 1.6M PEOPLE | NO ATTACKER NAMED | NO MISUSE SEEN (COMPANY)

SBC Medical Group: at least 1.6 million people exposed

KEY FACT **What happened.** Nasdaq-listed SBC Medical Group Holdings, which supports cosmetic and aesthetic clinics in Japan, told the SEC of two incidents on 16 November: an intrusion into databases behind a website system at its subsidiary SBC Medical Group, Ltd., and unauthorised access to clinic administrator accounts on the third-party Tribeau booking platform. [20][21]

DATA CATEGORY (DATABASE INCIDENT)	PEOPLE	YEARS
Basic personal information	1,624,000	2010–2023
Reservation requests (ad / campaign pages)	255,416	2007–2026
Website form inquiries	217,769	2004–2026
Reviews	15,007	2015–2018
Treatment-monitor information	4,513	2013–2026
Employee accounts (names, IDs, passwords)	~20,000	—

Table 3 · Counts from Exhibit 99.1 [21]. Categories may overlap, so they cannot simply be added; SecurityWeek's "over 2 million" sums them [22]. Tribeau: about 19,000 more people (12,641 and 6,804).

WHAT WAS IN IT

Names, sex, phone numbers, emails, passwords, addresses, dates of birth, patient card numbers, member IDs, survey answers, form contents, treatment descriptions and stored image file names (not the images). For 459 employees: bank, pension and tax details. Card data for 14 people was in old inquiry forms; the company says none of those cards still works. [21]

WHAT WAS NOT

Electronic medical records and the mySBC reservation site are not confirmed as accessed; clinical systems were out of scope. Japan's privacy regulator (PPC) was notified on 16 November. [21]

IF YOU ARE A PATIENT

- Change any password you reused from an SBC clinic website.
- Expect convincing phishing that mentions your treatment or booking.
- Clinics will not ask for card numbers or passwords by message or phone.

FOR SECURITY TEAMS

- Stored passwords and employee credentials: plan forced resets and watch for credential stuffing.
- Third-party booking admin accounts need MFA and their own access review.
- Old data is still data: inquiries back to 2004 were exposed. Set retention limits.

The company says it cannot yet estimate the financial impact. The intrusion method is under investigation. [20][21]

RUBY FIXED 18 NOV | PHP FIXED 19 NOV | NO ATTACKS REPORTED | CVSS VARIES BY SOURCE

Ruby2Shell and PHP: update the interpreter, not the app

RUBY **Ruby2Shell (CVE-2026-132825).** A one-byte heap overflow in Ruby's own String case conversion for single-byte encodings such as ISO-8859-1. Upcasing "ß" gives "SS": Ruby reserves one byte but writes two. One of seven Regexp/String flaws fixed on 18 November. [24][25]

RUBY BRANCH	VULNERABLE	FIXED
4.0	4.0.0–4.0.9	4.0.10
3.4	3.4.0–3.4.12	3.4.13
3.3	≤ 3.3.13	3.3.14
3.2 and older	end of life	no fix

- Credited to Stephan Lipp (Ada Logics) and Anthropic; the name comes from Veria Labs. [24][26]
- Severity conflicts: SecurityWeek gives CVSS 7.4; THN calls it critical. Ruby gives no score. [25][26]
- watchTowr says production RCE needs a non-glibc allocator, specific configuration and an ASLR bypass. SecurityWeek expects malformed requests mostly to cause crashes. [25]
- GitHub Enterprise Server is affected; GitLab and others have patched. [25][26]

PHP **PHP, 19 November.** 8.6.0 and 8.5.13 fix 7 critical and 10 high/medium bugs; most fixes are also in the older branches. No exploitation reported. [27][29]

PHP BRANCH	FIXED
8.6	8.6.0 (GA)
8.5	8.5.13
8.4	8.4.28
8.3	8.3.37
8.2	8.2.36

- CVE-2026-129289: PHP-FPM / LSAPI request smuggling, CVSS 9.2. [29]
- CVE-2026-115560: session deserialization RCE, but only if `session.serialize_handler` is changed at runtime. Stop-gap: `session.upload_progress.enabled=0`. [28]
- Two fixes (CVE-2026-129481, -129182) relate to October's widely exploited PHP2Shell. [29]

Linux · bash | user | READ-ONLY | NOT TESTED BY MAG212

CHECK

```
ruby -v
bundle exec ruby -v   # in app dir
docker run --rm IMAGE ruby -v
php -v
php -i | grep upload_progress.enabled
php -i | grep serialize_handler
```

MAG212 suggestion: standard version and setting checks to compare with the fixed releases [24, 27, 28]. Replace IMAGE with each of your images. Not run by MAG212.

WHY 'BUNDLE UPDATE' IS NOT ENOUGH

- Ruby2Shell lives in the interpreter binary. Gems and Rails updates do not touch it.
- Rebuild base images and redeploy; restart long-running workers.
- Ruby 3.2 apps are stuck: plan an upgrade. Veria Labs plans to publish its PoC about a week after disclosure. [26]
- PHP: update the PHP-FPM / mod_php package and restart the pool; app code changes do not help.
- Managed platforms (PaaS, hosted CI): confirm the provider has rolled the runtime.

Also today

CISA KEV · 18 NOV

Four exploited flaws added to KEV

Apache Axis 1.x CVE-2026-90436 (exploited against Confluence, per Rapid7; Axis 1 is end of life) and REDCap CVE-2026-90817 are due 21 November. LiteLLM CVE-2026-40217, used for "LLMjacking", is due 2 December. Synology DSM CVE-2024-10441 was used to deploy C3RB3R ransomware. We could not check KEV entries for 19–20 November. [30][31]

MSP · CLOUD INCIDENT

N-able confirms a cloud server breach

Unknown actors accessed one server in the Mail Assure and SpamExperts hosted cloud. Management UI, APIs, quarantine and logging are offline in three regions; mail flow still works. N-able sees no evidence of customer data access and says it is unrelated to the N-central flaws. [32][33]

FINANCE · THIRD PARTY

JPMorgan, Visa, Mastercard: vendor leak

After the N0n group's 16 November claims, all three cite incidents at unnamed vendors. Reuters found 16,000+ JPMorgan customer emails and some Visa records; Mastercard says a limited number of emails from one benefit programme. All say payment systems were unaffected. [34]

PATCH · CMS / OS

Drupal installer flaw; Windows 'FastUnlock'

Drupal fixed CVE-2026-132165, which lets an unauthenticated attacker re-run the installer on some setups (10.6.22, 11.3.22, 11.4.13). A public lock-screen bypass, FastUnlock, needs physical access, has no patch and does not break BitLocker. No attacks reported for either. [36][37]

ALSO NOTED

ITEM	WHY IT MATTERS	SEE
Nvidia: Gentlemen ransomware claim	Nvidia says a third-party partner may be affected; no impact on its systems	[35]
ROMULUS ClickFix campaign	Fake tool MSI and ChatGPT Custom GPT lures deliver a RAT using DoH C2	[38]
GTIG AI threat tracker	Autonomous offensive frameworks now seen in real intrusions	[42]

UPDATES ON YESTERDAY'S STORIES

ITEM	STATUS ON 20 NOV	SEE
nginx2root (CVE-2026-123007)	Censys PoC without huge traffic; ~9M exposed services; no attacks seen	[39]
Java4Shell (OpenJDK)	Attempts seen by GreyNoise, watchTowr, Cloudflare; no confirmed compromise	[40]
Equinor	Email reportedly down; production unaffected; no claim of responsibility	[41]
agent-framework PyPI	Maintainer confirms removal; investigation under way	Daily 19 Nov

Your work list for today

Ordered by urgency. Each row points to the page with evidence, commands and verification steps.

WHEN	TEAM	ACTION	SEE
TODAY	Virtualization	Patch vCenter (8.0 U3m / 9.0.2.0200 / 9.1.1.0200, VCF 5.2.5); restrict TCP 2012 to vCenter peers.	p.04
TODAY	SOC / IR	Hunt GTIG indicators: sps-* accounts, /tmp/123, /tmp/sss, /tmp/dbr, vmtoolscs, ports 53/33992.	p.04
TODAY	UC / network	Clustered Expressway to X15.5.20; allow 4371/4372 only between peers; grep for wombat.	p.05
48 H	Network	List all SonicWall Gen 6: WAN management off, SSL VPN off or restricted, MFA, reset passwords.	p.06
48 H	Platform	Upgrade Ruby interpreters (4.0.10 / 3.4.13 / 3.3.14) and PHP; rebuild images.	p.09
48 H	Vuln mgmt	KEV adds: Axis 1.x, REDCap (due 21 Nov), Synology DSM, LiteLLM.	p.10
THIS WEEK	Identity	If vCenter indicators hit: rotate STS signing certificate, reset SSO, review AD exposure.	p.04
THIS WEEK	Security lead	Budget and schedule Gen 6 replacement; ask partners about Secure Upgrade Plus.	p.06
THIS WEEK	Awareness	Warn staff about breach-themed phishing (SBC, JPMorgan/Visa vendor leak).	p.08 / 10
THIS MONTH	Architecture	Map management and cluster ports reachable from user networks; filter east-west.	p.12

ONE-PAGE HUNT SHEET

vCenter	`sps-*@vsphere.local`; SUID on `/bin/env`; SSH banner `pulsesecure_23345`.
Expressway	`wombat@127.0.0.1` in erlang.log; .py files under `/mnt/harddisk/i####/`.
Network	Traffic to 66.179.31[.]32, 18.130.47[.]116; listeners on 53/33992 on appliances.
SonicWall	Admin logins from the WAN; new local users; config changes outside change windows.
Runtimes	`ruby -v` below the fixed versions in any image or worker.

BEFORE YOU CLOSE A TICKET

- vCenter build matches the VMSA; TCP 2012 unreachable from user networks.
- Expressway on X15.5.20 on every cluster node.
- No Gen 6 with WAN management or open SSL VPN.
- ruby -v and php -v show fixed versions in production images.

COMMAND SAFETY

Every command in this issue is read-only. Sources: Ostorlab write-ups, Ruby and PHP guidance, or labelled MAG212 triage suggestions built from GTIG indicators. None was run by MAG212; test on one system first, and do not run network tests against systems you are not authorised to assess.

The devices nobody patches

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



A device nobody patches is a door nobody locks.

Know what you own, know when support ends, and replace it before that date.

Today: SonicWall Gen 6 retired · Expressway X14 must migrate · vCenter 7.0 has no public fix

Figure 4 · How end-of-life equipment becomes an entry point. Conceptual illustration, MAG212 CYBER [11, 12].

FOR EVERY EMPLOYEE

- Do not plug in old routers, firewalls or NAS boxes you find in a cupboard. Ask IT first.
- A home or branch device that "still works" may no longer get security fixes.
- If a company you use announces a breach, change any reused password and expect phishing that mentions it.
- Report odd login prompts or MFA requests you did not start.

FOR ADMINISTRATORS

- Keep an inventory with end-of-support dates, including spares and branch units.
- Management and cluster ports (vCenter 2012, Expressway 4372) belong on admin networks only.
- After a suspected compromise, patching is not cleanup: rotate keys and certificates the attacker could hold.
- Rebuild container images after runtime fixes like Ruby and PHP.

FOR BUSINESS LEADERS

- Unsupported edge devices are a business risk with a date on it. Fund replacement before that date.
- Ask for one list: internet-facing systems, owner, version, end-of-support date.
- Vendors and agencies now plan for AI-speed attacks. Patch windows measured in weeks are too slow for edge systems.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Which of our devices reach end of support in the next twelve months?
2. Can a laptop on the office network reach our vCenter or firewall management ports?
3. If a signing key were stolen, who would rotate it, and how long would it take?

Sources

[1] Broadcom · 19–20 Nov 2026 · VMSA-2026-0009.1: VMware vCenter Server, Cloud Foundation and Tools updates

[2] VMware (GitHub) · 19 Nov 2026 · VMSA-2026-0009 questions and answers

[3] Google GTIG / Mandiant · 19 Nov 2026 · ARMORY CASTLE exploits vSphere zero-day

[4] The Hacker News · 19 Nov 2026 · China-linked hackers exploit critical VMware vCenter flaw

[5] SecurityWeek · 19 Nov 2026 · Newly patched VMware vCenter flaw exploited as zero-day by Chinese APT

[6] Ostorlab · 19 Nov 2026 · VMware vCenter authentication bypass CVE-2026-123890

[7] Mandiant (GitHub) · accessed 20 Nov 2026 · vcsa-hardening-tool

[8] Cisco · 21 Oct 2026 · cisco-sa-vcs-static-cred-hr7EWZ8t: Expressway static credential vulnerability

[9] The Hacker News · 19 Nov 2026 · Hackers exploit critical Cisco Expressway flaw

[10] Ostorlab · 19 Nov 2026 · Cisco Expressway root RCE CVE-2026-76466

[11] SonicWall · 18 Nov 2026 · Product advisory: Retire unsupported Gen 6 firewalls

[12] The Hacker News · 20 Nov 2026 · SonicWall warns Gen 6 firewalls won't get patches

[13] SonicWall · 3 Nov 2026 · SNWLID-2026-0014: SonicOS 7.3.4 and 8.2.3 security advisory

[14] The Hacker News · 4 Nov 2026 · SonicWall won't patch end-of-life GMS flaws

[15] European Commission · 19 Nov 2026 · Midday press briefing (video I-298222)

[16] SecurityWeek · 20 Nov 2026 · European Commission confirms AI-assisted cyberattack disrupted services

[17] Help Net Security · 20 Nov 2026 · European Commission: AI-generated cyberattack used publicly available tool

[18] Computing · 20 Nov 2026 · European Commission hit by AI-assisted cyberattack

[19] BleepingComputer · 15 Nov 2026 · FBI warns ARTEX AI hacking tool is powering global cyberattacks

[20] SEC EDGAR · 18 Nov 2026 · SBC Medical Group Holdings Form 8-K

[21] SEC EDGAR · 18 Nov 2026 · Ex. 99.1: SBC Medical Group reports cybersecurity incidents in Japan

[22] SecurityWeek · 19 Nov 2026 · SBC Medical Group data breach impacts over 2 million

[23] SC Media · 19 Nov 2026 · SBC Medical Group discloses data breach affecting 1.6 million people

[24] ruby-lang.org · 18 Nov 2026 · Multiple vulnerabilities in Regexp and String case conversion

[25] SecurityWeek · 19 Nov 2026 · Ruby patches Ruby2Shell vulnerability that could lead to RCE

[26] The Hacker News · 19 Nov 2026 · Ruby releases fixes for 7 regex and string flaws

[27] PHP · 19 Nov 2026 · PHP 8 ChangeLog

[28] Aikido · 19 Nov 2026 · PHP security release, 19 November 2026 (CVE-2026-115560)

[29] SecurityWeek · 19 Nov 2026 · PHP patches seven critical RCE vulnerabilities

[30] The Hacker News · 19 Nov 2026 · CISA warns of 4 exploited flaws

[31] SecurityWeek · 19 Nov 2026 · Critical Apache Roller, Axis vulnerabilities exploited in attacks

[32] The Hacker News · 19 Nov 2026 · N-able confirms hackers accessed cloud server

[33] SecurityWeek · 20 Nov 2026 · N-able blames service disruption on cyberattack

[34] SecurityWeek · 20 Nov 2026 · JPMorgan, Visa, Mastercard cite third-party incidents amid data leak

[35] SecurityWeek · 19 Nov 2026 · Nvidia responds to Gentlemen ransomware claim

[36] The Hacker News · 19 Nov 2026 · Drupal patches critical installer flaw

[37] The Hacker News · 20 Nov 2026 · New unpatched Windows 0-day FastUnlock

[38] The Hacker News · 20 Nov 2026 · ROMULUS ClickFix attacks deliver RAT

[39] SecurityWeek · 19 Nov 2026 · F5 patches critical nginx2root flaws as PoC exploits go public

[40] SecurityWeek · 19 Nov 2026 · Java4Shell exploitation attempts begin as vendors rush out advisories

[41] The Record · 18 Nov 2026 · Norway's Equinor hit by cyberattack

[42] Google GTIG · 16 Nov 2026 · AI Threat Tracker: agentic threat activity crosses a significant threshold

[43] CERT-EU · 2 Apr 2026 · European Commission cloud breach: a supply-chain compromise

HOW WE VERIFIED THIS ISSUE

- Primary sources read: Broadcom VMSA-2026-0009.1 and FAQ, GTIG/Mandiant's ARMORY CASTLE report, Cisco's advisory, SonicWall's notices, the Commission briefing as reported, SBC's SEC 8-K and Exhibit 99.1, ruby-lang.org and php.net.
- F6's Expressway report did not load: exploitation details come from The Hacker News and Ostorlab. Politico's EC story was not fetched; ARTEX and service names are labelled as reported.
- cisa.gov could not be reached: KEV status is as reported by the cited outlets. Hunting commands are from Ostorlab or are labelled MAG212 suggestions.
- CVSS scores differ by scorer and are labelled. No command in this issue was executed by MAG212.

Read.
Verify.
Defend.

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

SUBSCRIBE FREE

Get every issue in your inbox

cyber.mag212.com/subscribe-free

MAG212 ATLAS · LIVE DEMO

Map every network before you test it

demo.atlas.mag212.com

WORK WITH MAG212 CYBER

Penetration testing
Find the forgotten edge before someone else does.

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

Training
For staff, IT teams, leaders and schools.

cyber.mag212.com/services

Watch the Atlas walkthrough: youtu.be/j27B5g3viKw

MAG212 CYBER

Daily · 20 November 2026
Understand the threat. Build the defense.