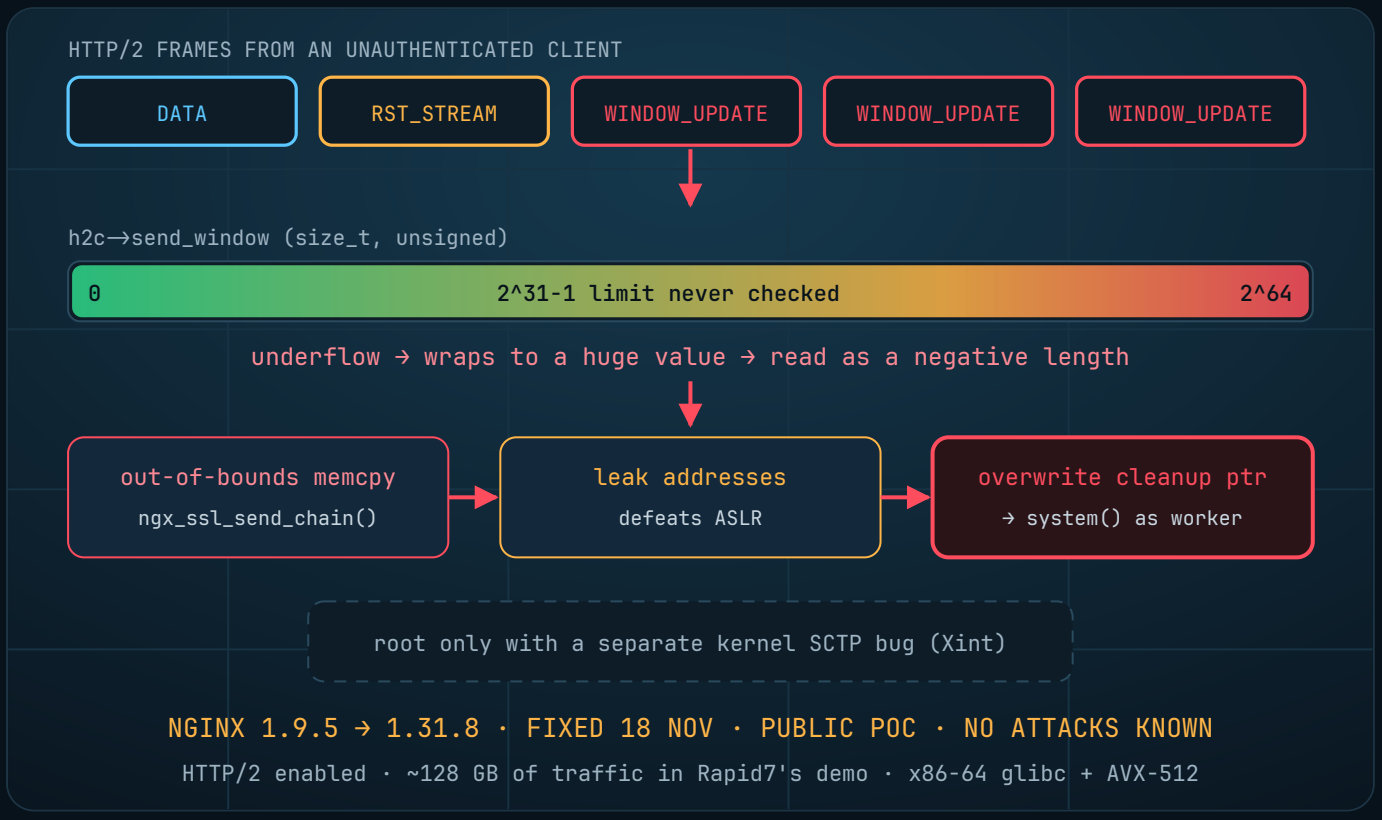
MAG212
CYBER

DAILY

Thursday, 19 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 6:00 AM PT



NGINX2ROOT · CVE-2026-123007

A ten-year-old counter

Since 2015, nginx's HTTP/2 code could be tricked into handing back flow-control credit twice. Three teams turned that into code execution without a login, and a public exploit is out. Also today: Apache Roller is under attack, and F5 ships hotfixes for six critical BIG-IP flaws.

03 nginx2root: how a counter becomes RCE
05 F5 BIG-IP: six 9.8 TMM overflows
06 Apache Roller RCE is being exploited
07 Microsoft's agent-framework hijacked on PyPI
08 EggStreme rebuilt: the agent that listens
09 Cold Relic turns a victim into a lure

1.31.9
nginx mainline fix · 1.30.7 stable

9.2
CVSS 4.0 for nginx2root (F5)

6 × 9.8
BIG-IP TMM overflows, hotfix only

EXPLOITED
Apache Roller XML-RPC, per Apache

What matters today

Developments published or updated 17–19 November. The Roller flaw was first fixed in September; it is included because Apache confirmed exploitation and widened the affected range on 17 November.

Web edge, patch night

nginx 1.31.9 and 1.30.7 fix nginx2root and four other worker memory bugs. F5 also shipped hotfixes for six critical BIG-IP flaws that need specific iRules or APM policies. Neither is known to be exploited. [1] [2][9]

Exploited now: Apache Roller

Apache says its Roller blog server's pre-auth XML-RPC deserialization bug “is being actively exploited”. A re-issued CVE widens the range back to Roller 4.0.0. [11][15]

Signed, then poisoned

Two releases of Microsoft's official agent-framework package on PyPI stole cloud and CI tokens for about an hour on 17 November. They were published with a stolen release-pipeline credential. [16][17]

Quiet espionage

EggStreme's operators rebuilt their malware after exposure; some agents now only listen on TCP 5060. A Russian group reused a victim's identity to phish the next target. [18][21]

THE THREE PRIORITY ACTIONS

1. **Patch nginx to 1.31.9 / 1.30.7 (or your distro’s fix) and fully restart it.**
   A reload leaves the old binary running. If you cannot patch yet, turn HTTP/2 off on internet-facing listeners. Check NGINX Plus, ingress and appliance vendors separately. [1][7]

2. **Upgrade Apache Roller to 6.1.7, or cut off XML-RPC today.**
   Set `enabledForExtensions` to false in WEB-INF/web.xml or remove the servlet mapping, then restart. Treat exposed servers as possibly compromised. [11][14]

3. **If agent-framework 1.26.1 or 1.26.2 was installed anywhere, rotate every secret it could see.**
   Pin to 1.26.0, look for the two .pth files, and revoke Azure, GitHub, DevOps, npm, PyPI and Docker tokens on those machines and CI runners. [16]

CONTENTS

03 nginx2root: how a counter becomes RCE
04 nginx2root: check, patch, detect
05 F5 BIG-IP: six critical TMM flaws
06 Apache Roller: exploited XML-RPC RCE
07 agent-framework PyPI hijack
08 EggStreme: rebuilt to stay quiet
09 Cold Relic: the borrowed identity
10 Briefs
11 Defender's Action Desk
12 Awareness: when a partner messages you
13 Sources

FIXED 18 NOV | CVSS 4.0 9.2 · 3.1 8.1 (UBUNTU) | PUBLIC POC (RAPID7) | NO KNOWN EXPLOITATION

nginx2root: how a ten-year-old counter becomes RCE

KEY FACT **What happened.** On 18 November nginx released 1.31.9 and 1.30.7, fixing CVE-2026-123007, a memory-corruption bug in HTTP/2 flow control present since 1.9.5 (September 2015). Xint, Rapid7 and Wiz each found it independently and each achieved code execution as the nginx worker user without logging in. [1][3][4] [5][6]

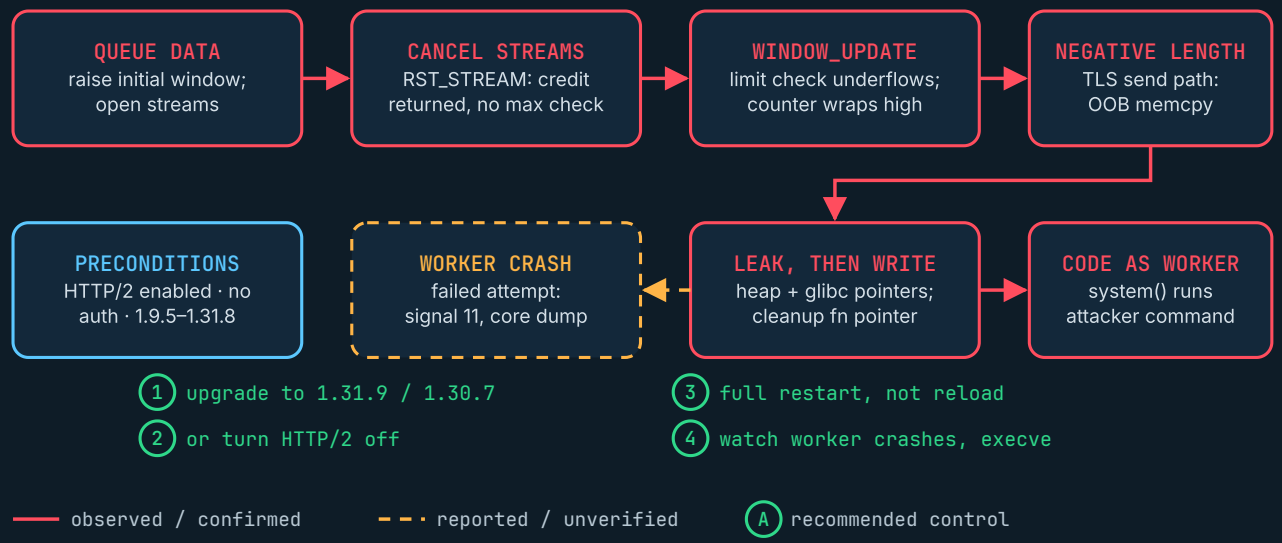


Figure 1 · nginx2root attack path, from Rapid7's and Xint's write-ups. Red = described by the researchers; amber dashed = failure path. Diagram: MAG212 CYBER.

HOW THE ATTACK WORKS

When a client cancels streams that still have DATA queued, `ngx_http_v2_filter_cleanup()` gives the credit back to the connection's send window without checking the 2^31−1 ceiling. A later WINDOW_UPDATE check then underflows, and nginx keeps the connection open where the HTTP/2 spec says it should close it. The huge window is later treated as a negative length, and `ngx_ssl_send_chain()` copies past its buffer. [4][6]

Rapid7's proof of concept uses that copy first to leak heap and glibc addresses, defeating ASLR, then to redirect a pool cleanup callback to `system()`. Root needs a second, separate bug: Xint chained a Linux kernel SCTP flaw that has no CVE yet. [4][6][7]

WHAT IT TAKES

- HTTP/2 enabled (`listen … http2` or `http2 on`). Serving static files is enough; no special module needed. [5]
- Rapid7's demo pushed about 128 GB in ~2.5 minutes: about 17 minutes at 1 Gbit/s. Below ~300 Mbit/s the one-hour connection limit gets in the way. [4]
- The demonstrated exploit relies on x86-64 glibc's AVX-512 memcpy. Other platforms are not shown exploitable for RCE; treat them as crashable. [4]
- A CDN or load balancer that terminates HTTP/2 may blunt the attack. Test the origin directly. [4][5][7]

EXPLOITATION STATUS

No attacks reported and not in CISA KEV as of 18 November. Rapid7's PoC is public but built for a fresh local Docker container; Wiz and Xint are withholding theirs. [1][4][5]

nginx2root: check, patch, detect

The same release fixes four more worker memory bugs: CVE-2026-123633, 123634, 121810 and 113425.

PRODUCT	VULNERABLE	FIXED
nginx open source (mainline)	1.31.0-1.31.8	1.31.9
nginx open source (stable)	1.9.5-1.30.6	1.30.7
NGINX Plus	37.1.0-37.2.0.1	37.3.0.1
NGINX Plus	37.0.0-37.0.7.1	37.0.8.1
NGINX Plus	R34-R36	no fix listed: move to 37.x or disable HTTP/2

Table 1 · Versions from Rapid7 and The Hacker News [1, 4]; nginx.org advisory [2]; Ubuntu listed all releases vulnerable on 18 Nov [8]. F5's K000163926 did not load for us: confirm on F5's site.

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

VERSION + HTTP/2 CHECK

```
nginx -v 2>&1
sudo nginx -T 2>&1 | sed 's/#.*//' \
  | grep -nE 'listen.*http2|http2
+on|listen.*quic'
openssl s_client -connect
example.org:443 \
  -servername example.org -alpn h2 &1 \
  | grep -E 'ALPN protocol|No ALPN'
```

From CIRCL TR-105. Backported distro fixes keep old version strings. `ALPN protocol: h2` means HTTP/2 is live on that listener. Do not publish raw `nginx -T` output: it contains your whole config. [7]

nginx.conf | web admin | CHANGES SYSTEM | NOT TESTED BY MAG212

WORKAROUND

```
server {
    listen 443 ssl;      # 'http2'
removed
    http2 off;           # nginx ⩾
1.25.1
    # existing configuration
}
sudo nginx -t && sudo systemctl restart
nginx
```

Temporary workaround from CIRCL and Wiz. Change every server block sharing the listener, IPv6 included. Covers 123007 and 123633 only; breaks gRPC. Restart, do not reload: a reload keeps the old binary. [5][7][1]

WHAT TO LOOK FOR

- `worker process … exited on signal 11` or segfault lines in error.log; nginx entries in `coredumpctl list nginx`. [7]
- Long-lived :443 connections with very large inbound bytes but few logged requests. WINDOW_UPDATE and RST_STREAM frames never appear in access logs. [6][7]
- Child processes of nginx workers (`execve` by the worker UID in auditd). [6]
- No public network signature exists.

CONTAIN, FIX, VERIFY

1. List every nginx: hosts, containers, ingress controllers, appliances. Note which negotiate h2.
2. Upgrade (or disable HTTP/2), then fully restart and rebuild images.
3. Ask NGINX Plus, ingress and appliance vendors for their own fix status.
4. Verify: fixed package version, and ALPN no longer h2 where you turned it off.
5. No SCTP needed? Block the module (CIRCL).

PUBLISHED 18 NOV | CVSS 3.1 9.8 · 4.0 9.3 | HOTFIX ONLY · NO WORKAROUND | NO KNOWN EXPLOITATION

F5 BIG-IP: six critical flaws, each behind one setting

KEY FACT What happened. F5 disclosed six stack buffer overflows in TMM, the BIG-IP data plane. An unauthenticated attacker sending crafted traffic can crash TMM, interrupting traffic until it restarts, and may run code. Each needs a specific iRule command or APM policy. watchTowr's Sina Kheirkhah reported four; F5 found two. They are part of a 22-advisory batch. [9][10]

CVE	VULNERABLE ONLY IF A VIRTUAL SERVER HAS…	PRODUCTS
CVE-2026-123637	APM per-request policy with both Client Information and Endpoint Security agents	BIG-IP APM
CVE-2026-121805	iRule using `PEM::subscriber` on client traffic	BIG-IP (PEM), BNK, CNF
CVE-2026-120292	HTTP profile + iRule using `MR::message route`	BIG-IP (all modules), BNK
CVE-2026-120285	HTTP profile + iRule using `PSC::ip_address`	BIG-IP (all modules), BNK, CNF
CVE-2026-116953	iRule using `GENERICMESSAGE::route` on client traffic	BIG-IP (all modules), BNK
CVE-2026-120722	iRule using `DNS::scrape` on client traffic	BIG-IP DNS, BNK; CNF disputed

Table 2 · Trigger configurations from The Hacker News and Censys [9, 10]. F5's own K-articles did not load for us; CNF status of CVE-2026-120722 conflicts between F5's advisory and the CVE record.

BRANCH	ENGINEERING HOTFIX (PER F5 RECORDS VIA CENSYS)
BIG-IP 21.1.0	BIGIP-21.1.0.4.0.19.3-ENG
BIG-IP 17.5.0	BIGIP-17.5.1.11.0.61.12-ENG or 17.5.1.10.0.80.35-ENG
BIG-IP 17.1.0	BIGIP-17.1.3.7.0.21.4-ENG or 17.1.3.6.0.14.20-ENG
BNK / CNF 2.2–2.4	BNK-2.4.2-EHF1 · 2.3.4-EHF1 · 2.2.5-EHF1 (CNF: same numbering)

WHY IT MATTERS

- F5 lists no workarounds, and hotfixes skip full QA; F5 says they carry no warranty. [9]
- Versions outside technical support were not evaluated: absence from F5's table is not a clean bill. [9][10]
- A different APM overflow (CVE-2026-94127) went into CISA KEV in September. Expect researchers to look at these too. [9]

BIG-IP · tmsh / bash | admin | READ-ONLY | NOT TESTED BY MAG212

IRULE TRIAGE

```
tmsh list ltm rule one-line \
  | grep -E
'PEM::subscriber|MR::message|PSC::ip_add
ress|\
GENERICMESSAGE::route|DNS::scrape'
tmsh list ltm virtual rules
```

MAG212 triage suggestion, not an F5 procedure: list iRules that use the five trigger commands, then which virtual servers attach them. A match means the hotfix is urgent; no match lowers but does not remove the priority. Review APM per-request policies by hand. [9][10]

ACTIVELY EXPLOITED (APACHE) | CVSS 3.1 9.8 | PUBLIC EXPLOIT TOOL

KEV: NOT LISTED AS OF 17 NOV

Apache Roller: the blog server bug attackers are using

KEY FACT **What happened.** On 17 November the Roller project published CVE-2026-129448 and stated: "This issue is being actively exploited." It is the same pre-auth Java deserialization flaw as September's CVE-2026-82384, which listed only 6.1.5 as affected. The new record covers Roller 4.0.0 to 6.1.4. [11][12][15]

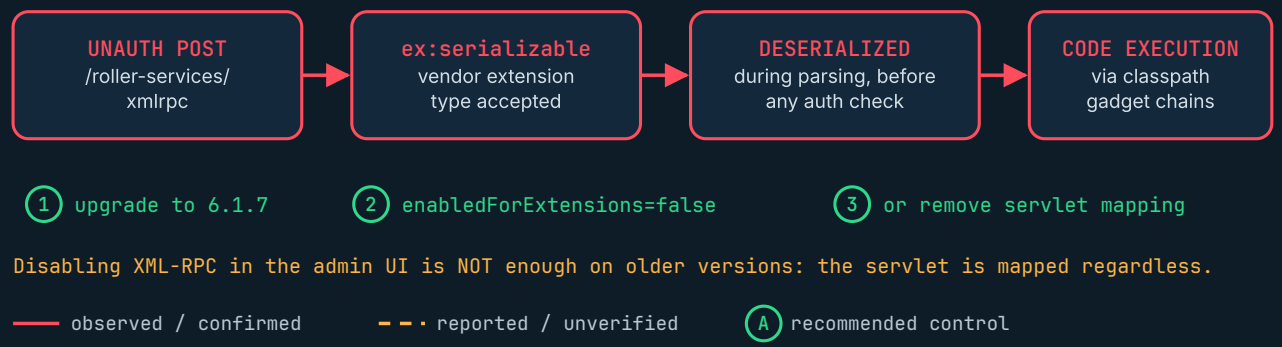


Figure 2 · Roller XML-RPC deserialization path per Apache's advisories and Corgea's analysis [11, 12, 14]. Diagram: MAG212 CYBER.

WHAT WE KNOW

- Affected: 4.0.0–6.1.4 (CVE-2026-129448) and 6.1.5 (CVE-2026-82384). Fixed from 6.1.6. [11][12]
- Target 6.1.7 (11 Nov): it fixes 15 more CVEs, including another deserialization bug (CVE-2026-123374) that affects 6.1.6. Read its release notes; some changes affect existing sites. [13][32]
- Apache named no attacker, victim or payload. No network IoCs are public. [15]
- An open exploit framework for CVE-2026-82384 has been on GitHub since late September; it ships no gadget chain. [14]

WHY SCANNERS MISSED IT

Our reading, not Apache's: tools that trusted September's "6.1.5 only" record would have marked older, long-lived Roller installs as safe for two months. [12][14]

WEB-INF/web.xml | app admin

CHANGES SYSTEM | NOT TESTED BY MAG212

WORKAROUND

```
<init-param>
  <param-
name>enabledForExtensions</param-name>
  <param-value>false</param-value>
</init-param>
```

Apache's official workaround if you cannot upgrade yet. Alternatively, delete the /roller-services/xmlrpc servlet mapping. Restart Roller afterwards. [11]

HUNT

- POSTs to `/roller-services/xmlrpc` whose body contains `ex:serializable` or `rO0AB`.
- Tomcat's JVM starting sh, bash, curl, wget, python or powershell.
- New `.jsp` files under webapps/; unexpected Roller admins. [14]

17 NOV · ~1 HOUR LIVE | STOLEN SIGNING CREDENTIAL | SAFE: 1.26.0

MICROSOFT STATEMENT: NONE FOUND

Microsoft's agent-framework: an hour of poisoned releases

KEY FACT **What happened.** Malicious versions 1.26.1 and 1.26.2 of Microsoft's official `agent-framework` package were on PyPI for about an hour on 17 November. Wiz says the attacker appears to have held a certificate and private key for Microsoft's ESRP release pipeline; how it was obtained is unknown. [16][17]

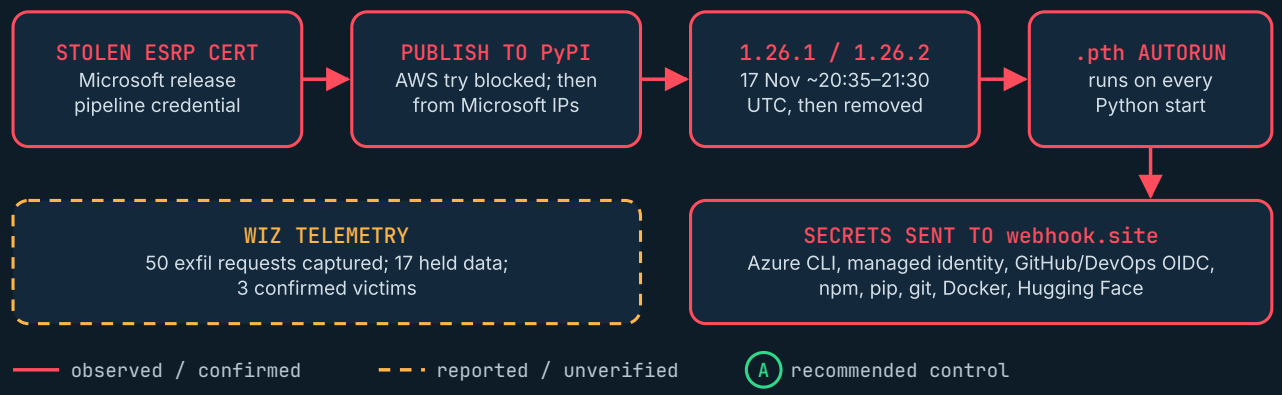


Figure 3 · Compromise chain per Wiz's analysis [16]. Red = reported by Wiz; amber dashed = telemetry. Diagram: MAG212 CYBER.

WHY IT IS NASTY

A `.pth` file in site-packages runs whenever Python starts, so the payload fired even where the package was installed but never imported, for example in a CI runner that pulled a fresh dependency. It harvested secret-looking environment variables, local tool credentials, CI OIDC tokens and Azure managed-identity tokens for 12 resources. [16]

The tooling calls itself "Cairn", an open-source AI pentest framework. Wiz has not attributed the attack. [16][29]

INDICATORS

FILES	`agent_framework_meta.pth` · `af_runtime_diag.pth`
VERSIONS	`agent-framework 1.26.1` · `1.26.2` (PyPI)

Linux / macOS · bash | user | READ-ONLY

NOT TESTED BY MAG212

CHECK

```
pip show agent-framework 2>/dev/null |
grep Version
python3 -c 'import site,glob;[print(f) \
  for d in site.getsitepackages() \
  for f in glob.glob(d+"/*.pth")]' \
  | grep -E
'agent_framework_meta|af_runtime_diag'
```

Shows the installed version and whether either malicious .pth file is present in the interpreter's site-packages. Repeat per virtualenv, image and CI cache. [16]

IF YOU FIND IT

1. Pin to 1.26.0 and rebuild environments and images.
2. Rotate every credential the host or runner could reach: Azure, GitHub, Azure DevOps, npm, PyPI, Docker, Hugging Face.
3. Azure tokens may remain valid up to 24 hours: revoke sessions, not just keys.
4. Review cloud audit logs from 17 Nov 20:35 UTC on.

BITDEFENDER · 18 NOV | SUSPECTED CHINA-NEXUS | PHILIPPINE GOVERNMENT | IoCs: MD5 + NETWORK

EggStreme rebuilt: the agent that waits for a call

KEY FACT **What happened.** Bitdefender reports that after its September 2025 exposé, EggStreme's operators re-engineered the framework rather than just rotating infrastructure: new loader and config ciphers, a new transport, new commands, and passive agents that never beacon. Victims are multiple Philippine government bodies; Taiwan is a lower-confidence lead. [18][20]

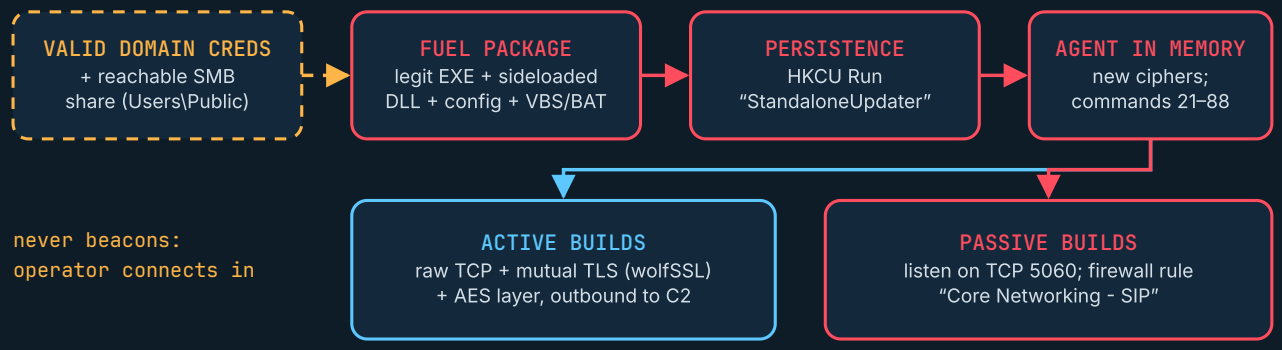


Figure 4 · EggStreme v2 chain per Bitdefender [18]. Initial access is unknown. Diagram: MAG212 CYBER.

WHAT CHANGED

- Loader: XOR → RC4 → RC5-32 → two custom CBC ciphers between Oct and Dec 2025. Fuel config moved to AES-256-CBC. [18]
- Agent: gRPC over mTLS replaced by raw TCP with mutual TLS (wolfSSL) plus AES. New commands add AD recon, WMI, token impersonation, in-memory .NET/PowerShell and a PE stager. Keylogger dropped. [18][20]
- Passive builds (compiled 2 Sep and 5 Nov 2025) open TCP 5060 and add an inbound rule named "Core Networking - SIP" to look like Windows VoIP defaults. [18]
- Attribution stays "suspected Chinese APT"; Bitdefender calls this a technical assessment. [18]

HOST INDICATORS (BITDEFENDER)

RUN KEY	`HKCU\…\Run StandaloneUpdater`
EXE	`%LOCALAPPDATA%\Microsoft\OneDrive\setup\logs\StandaloneUpdater.exe`
SCRIPTS	`C:\Users\Public\Officelog.bat` · `prncnfg.vbs`
DLL NAMES	`advapi32, dbghelp, dwmapi, iscsiexe, DevicesPlatform, xwizards (from non-system dirs)`
CONFIG	`%LOCALAPPDATA%\Microsoft\Windows\Notifications\wpndatabase.dat`
NETWORK	`fsstore[.]org` · `rodosdeals[.]com` · `mepintei[.]com` · `45[.]115[.]225[.]73` …

Full list: 101 rows in Bitdefender's GitHub CSV [19], MD5 only. Hashes change with every build; hunt the behaviours.

DEFENDER CHECKLIST

- Alert on a "Core Networking - SIP" rule and on new TCP 5060 listeners on hosts that are not VoIP systems.
- Detect system-library DLL names loaded from non-system folders; restrict WScript, attrib and reg where roles allow.
- Inventory unmanaged hosts that reach workstations over SMB. Capture process memory before cleanup: Fuel's RC4 key lives only in RAM. [18]

GTIG VIA SECURITYWEEK / THN | FSB-LINKED (US GOV) | NO IoCs PUBLISHED | PRIMARY POST NOT READ

Cold Relic: yesterday's victim is today's lure

KEY FACT **What happened.** Google's threat intelligence group described two intrusions by Cold Relic, the group also tracked as COLDRIVER and Star Blizzard. After being evicted from one US organisation, it posed as that organisation's employees to phish their contacts, and breached a second US organisation that way. [21][22]

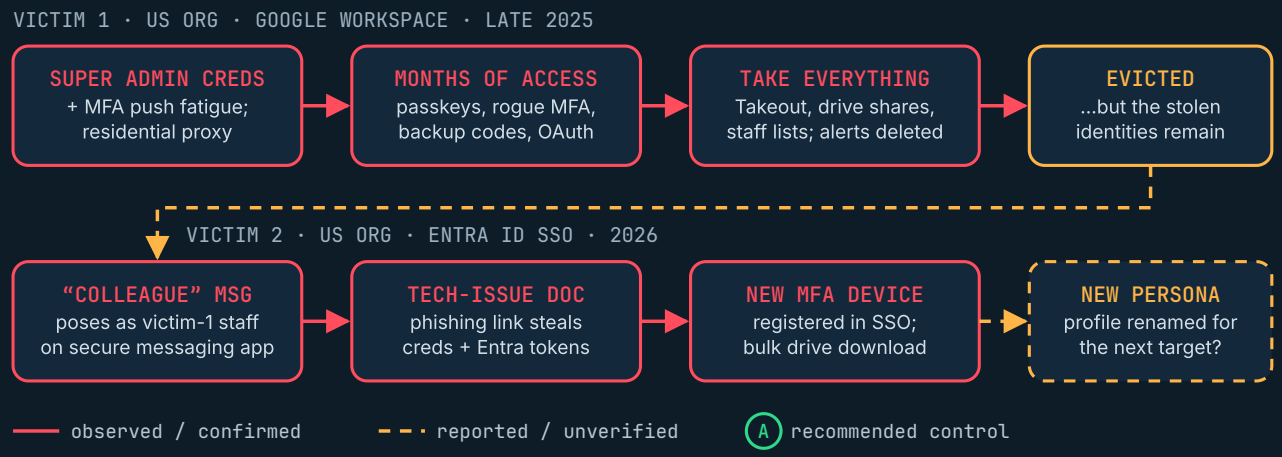


Figure 5 · Two-victim chain as summarised by SecurityWeek and The Hacker News [21, 22]. We could not load Google's original post; treat details as second-hand. Diagram: MAG212 CYBER.

WHAT IS DIFFERENT

No malware is named. Everything ran on built-in cloud features: the admin console, Google Takeout, OAuth mail sync, passkeys and MFA device registration. Passkeys that were never revoked survived password and session resets. The attackers also read audit logs to judge what defenders could see and deleted Alert Center notifications. [22]

The messaging app used against victim 2 is not named in the coverage, and neither victim is identified. [21][22]

WHAT TO DO (OUR TAKEAWAYS)

- Eviction means revoking passkeys, MFA devices, backup codes and OAuth grants, not only resetting passwords.
- Alert on Alert Center deletions and on admin use of Takeout; restrict Takeout where it is not needed.
- Use phishing-resistant MFA for admins; number matching at minimum against push fatigue.
- After a partner is breached, treat its staff's messages, especially on new channels, as untrusted until verified by phone.
- These are MAG212 inferences from the reported facts, not GTIG's published guidance. [22]

Also today

RESEARCH · INTRUSION

Japan’s Fugaku supercomputer offline after intrusion

RIKEN says an intruder got in through Fugaku's public operational-status dashboard between 10 and 13 November, reached internal servers and planted malware aimed at user data. Names, emails and user IDs of 4,222 Fugaku users and 375 users of the Rikyu system were exposed, along with SSH keys and files on users' machines. RIKEN shut Fugaku down on 14 November; it has named no vulnerability or attacker. [23]

ENERGY · ONGOING INCIDENT

Equinor fighting an ongoing cyberattack

Norway's Equinor said on 17 November it had detected an ongoing cyberattack on some IT systems, with no evidence of data theft or impact on operations, according to Reuters as reported by Gulf News. It notified authorities and mobilised resources to contain it. There is no attribution. We could not retrieve Equinor's own statement. [24]

JAVA · UPDATE

Java4Shell: exploitation attempts begin

Update to yesterday's lead. A SecurityWeek headline on 19 November reports exploitation attempts; we have not read who observed them. On 18 November CISA urged immediate patching but saw no exploitation, and Cloudflare shipped WAF detections while seeing no exploits. Not in CISA KEV. Treat as “attempts”, not confirmed compromises. [26][27][28]

PATCH · LANGUAGE RUNTIMES

PHP and Ruby security releases

PHP warned of critical flaws in all supported branches, with releases due 19 November that include CVE-2026-115560, a conditional remote code execution bug in session upload handling. Ruby 4.0.10, 3.4.13 and 3.3.14 fix seven regex and string flaws, five with code-execution proofs of concept. No attacks reported for either. Check the projects' pages for final version numbers. [25][30]

ALSO NOTED

ITEM	WHY IT MATTERS	SEE
Google: AI exploit frameworks in real attacks	Artex, Cairn, exploit_agent built and ran exploits without humans	[29]
TPM lockout bypass via flash chip	Short Windows Hello / BitLocker PINs crackable; AMD confirms flaw	[31]
F5 batch: 16 more advisories	10 for NGINX, plus iControl SOAP/REST fixes	p.05

STILL OPEN FROM EARLIER ISSUES

ITEM	STATUS ON 19 NOV	SEE
Puppet CVE-2026-115731 (KEV)	CISA deadline 1 December	Daily 18 Nov
OPTIMJACK script hijack	No root-cause update found	Daily 18 Nov
Copeland XWEB EVO: unfixed flaws	Unchanged; isolate and replace	Daily 17 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	Web / platform	Upgrade nginx to 1.31.9 / 1.30.7 or distro fix; full restart; rebuild images. Else turn HTTP/2 off.	p.04
TODAY	App owners	Apache Roller: upgrade to 6.1.7 or disable XML-RPC extensions; treat exposed servers as suspect.	p.06
TODAY	Dev / CI	Search for agent-framework 1.26.1/1.26.2; pin 1.26.0; rotate every reachable secret.	p.07
48 H	Network	Grep BIG-IP iRules for the five trigger commands; schedule F5 engineering hotfixes.	p.05
48 H	Platform	Ask NGINX Plus, ingress and appliance vendors for nginx2root fix status.	p.04
48 H	SOC	Alert on nginx worker crashes and child processes; Roller xmlrpc POSTs with rO0AB.	p.04 / 06
THIS WEEK	Endpoint	Hunt “Core Networking - SIP” firewall rules and TCP 5060 listeners on non-VoIP hosts.	p.08
THIS WEEK	Identity	Audit admin passkeys, MFA devices, OAuth grants; alert on Alert Center deletions and Takeout.	p.09
THIS WEEK	App / platform	Java4Shell: finish patching Java on x86-64 AVX-512 hosts; attempts reported.	p.10
THIS MONTH	Security lead	Review how fast release-pipeline signing credentials can be revoked and rotated.	p.07

ONE-PAGE HUNT SHEET

nginx	`signal 11` in error.log; huge-inbound :443 sessions.
Roller	xmlrpc POSTs with `rO0AB`; Tomcat → shell.
Python	`agent_framework_meta.pth`, `af_runtime_diag.pth` in site-packages.
Windows	Run value `StandaloneUpdater`; rule “Core Networking - SIP”; 5060 listener.
Cloud ID	New MFA devices or passkeys on admins; Takeout exports; deleted Alert Center items.

BEFORE YOU CLOSE A TICKET

- Roller on 6.1.7, or web.xml change confirmed and Roller restarted.
- No 1.26.1/1.26.2 in any lockfile, image or CI cache; secrets rotated.
- BIG-IP hotfix version confirmed on every unit in the HA pair.

COMMAND SAFETY

Commands in this issue are read-only except the nginx and Roller configuration changes, which alter behaviour and need a restart. Sources: CIRCL, Apache, Wiz, or labelled MAG212 suggestions. None was run by MAG212; test on one system first.

When a partner messages you out of the blue

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



A familiar name is not proof of a familiar person.

Verify through a channel you already had: call the number you have on file.

Cold Relic used real employees' identities, stolen in an earlier breach, to reach their contacts.

Figure 6 · How borrowed-identity phishing works, based on the Cold Relic case [21, 22]. Conceptual illustration, MAG212 CYBER.

FOR EVERY EMPLOYEE

- A known contact writing from a new app, number or address, about a “document” or “technical issue”, is a moment to pause.
- Check with a call to the number you already have, not one in the message.
- Never approve an MFA prompt you did not start. Repeated prompts mean someone has your password: report it.
- If you signed in through a link and then had doubts, tell IT now so they can revoke the session.

FOR ADMINISTRATORS

- Removing an intruder means removing their passkeys, MFA devices, backup codes and OAuth apps too.
- Watch for new MFA devices on admin accounts and for deleted security alerts.
- Developers: a package you trust can still ship a bad release. Pin versions and keep CI secrets short-lived.
- Restart services after patching: nginx keeps old code running after a reload.

FOR BUSINESS LEADERS

- When a supplier tells you it was breached, warn your staff that its people's names may be used against them.
- Ask which of our internet-facing systems run nginx, BIG-IP or old Java apps, and who restarts them tonight.
- Today's Roller case shows an old CVE record can understate who is exposed. Ask for asset lists, not scanner verdicts.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. If a partner's employee messaged us on a new app, how would we check it is really them?
2. Who can revoke every sign-in method on an account, and how long does it take?
3. Which third-party packages could reach our cloud credentials if one release went bad?

Sources

[1] The Hacker News · 18 Nov 2026 · 10-Year-Old NGINX HTTP/2 Flaw Lets Unauthenticated Attackers Execute Code on Servers

[2] nginx.org · 18 Nov 2026 · nginx security advisories

[3] nginx.org · 18 Nov 2026 · Changes with nginx 1.31.9

[4] Rapid7 (S. Fewer) · 18 Nov 2026 · CVE-2026-123007: Critical NGINX HTTP/2 integer underflow leads to RCE (fixed)

[5] Wiz Research · 18 Nov 2026 · NGINX HTTP/2 RCE vulnerabilities

[6] Xint (Theori) · 18 Nov 2026 · nginx2root: remote code execution

[7] CIRCL · 18 Nov 2026 · TR-105 NGINX2ROOT (TLP:CLEAR)

[8] Ubuntu · 18 Nov 2026 · CVE-2026-123007

[9] The Hacker News · 18 Nov 2026 · F5 Warns 6 Critical BIG-IP Flaws Can Crash Traffic in Specific Setups, May Allow RCE

[10] Censys · 18 Nov 2026 · Nov 18 Advisory: F5 BIG-IP iRule and APM TMM Remote Code Execution

[11] Apache Roller PMC (oss-security) · 17 Nov 2026 · CVE-2026-129448: XML-RPC deserialization, actively exploited

[12] Apache Roller PMC (oss-security) · 25 Sep 2026 · CVE-2026-82384: XML-RPC deserialization in 6.1.5

[13] Apache Roller PMC (oss-security) · 11 Nov 2026 · Apache Roller 6.1.7: 15 CVEs fixed

[14] Corgea Research · 17 Nov 2026 · CVE-2026-129448 / 82384: Apache Roller XML-RPC deserialization exploited

[15] SecurityWeek · 19 Nov 2026 · Critical Apache Roller, Axis Vulnerabilities Exploited in Attacks

[16] Wiz Research · 18 Nov 2026 · Malicious version of Microsoft's agent-framework published to PyPI

[17] The Hacker News · 18 Nov 2026 · Attackers compromise Microsoft's agent-framework PyPI package

[18] Bitdefender (B. Zavadovschi) · 18 Nov 2026 · EggStreme Malware: Rebuilt Under Scrutiny

[19] Bitdefender (GitHub) · 18 Nov 2026 · 2026_11-eggstreme-iocs.csv

[20] The Hacker News · 18 Nov 2026 · New EggStreme Malware Variant Goes Silent to Evade Security Tools in Government Attacks

[21] SecurityWeek · 18 Nov 2026 · Russian APT Poses as Employee of Hacked Firm to Breach Another US Organization

[22] The Hacker News · 18 Nov 2026 · Russian COLD RELIC Hackers Use Stolen Google Workspace Data to Breach Second U.S. Organization

[23] BleepingComputer · 17 Nov 2026 · Japan takes Fugaku supercomputer offline after cyberattack

[24] Gulf News (citing Reuters) · 17 Nov 2026 · Norway's Equinor detects cyberattack on IT systems, operations unaffected

[25] The Hacker News · 19 Nov 2026 · PHP warns of critical security flaws

[26] The Hacker News · 18 Nov 2026 · CISA urges immediate patching of Java4Shell

[27] Cloudflare · 18 Nov 2026 · Java4Shell (Zero-Wire)

[28] SecurityWeek · 19 Nov 2026 · Java4Shell Exploitation Attempts Begin as Vendors Rush Out Advisories (headline)

[29] SecurityWeek · 17 Nov 2026 · AI Framework Autonomously Weaponized Flaws in Real Attacks, Google Says

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

[31] The Hacker News · 18 Nov 2026 · Flash-chip attack bypasses TPM lockout

[32] Apache Security · accessed 19 Nov 2026 · Apache Roller project security advisories

HOW WE VERIFIED THIS ISSUE

- Primary sources read: nginx.org advisories and CHANGES, Rapid7, Wiz, Xint and CIRCL write-ups, Ubuntu's CVE page, Apache Roller's oss-security advisories, Wiz's agent-framework analysis, Bitdefender's EggStreme report and IoC CSV.
- F5's K-articles and Google's Cold Relic post did not load for us. F5 details come from The Hacker News and Censys; Cold Relic from SecurityWeek and The Hacker News. Equinor's statement is as reported by Reuters via Gulf News; the Java4Shell attempts item is from a SecurityWeek headline.
- cisa.gov could not be reached: KEV status is as reported by the cited outlets on the dates shown.
- 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 · 19 November 2026
Understand the threat. Build the defense.