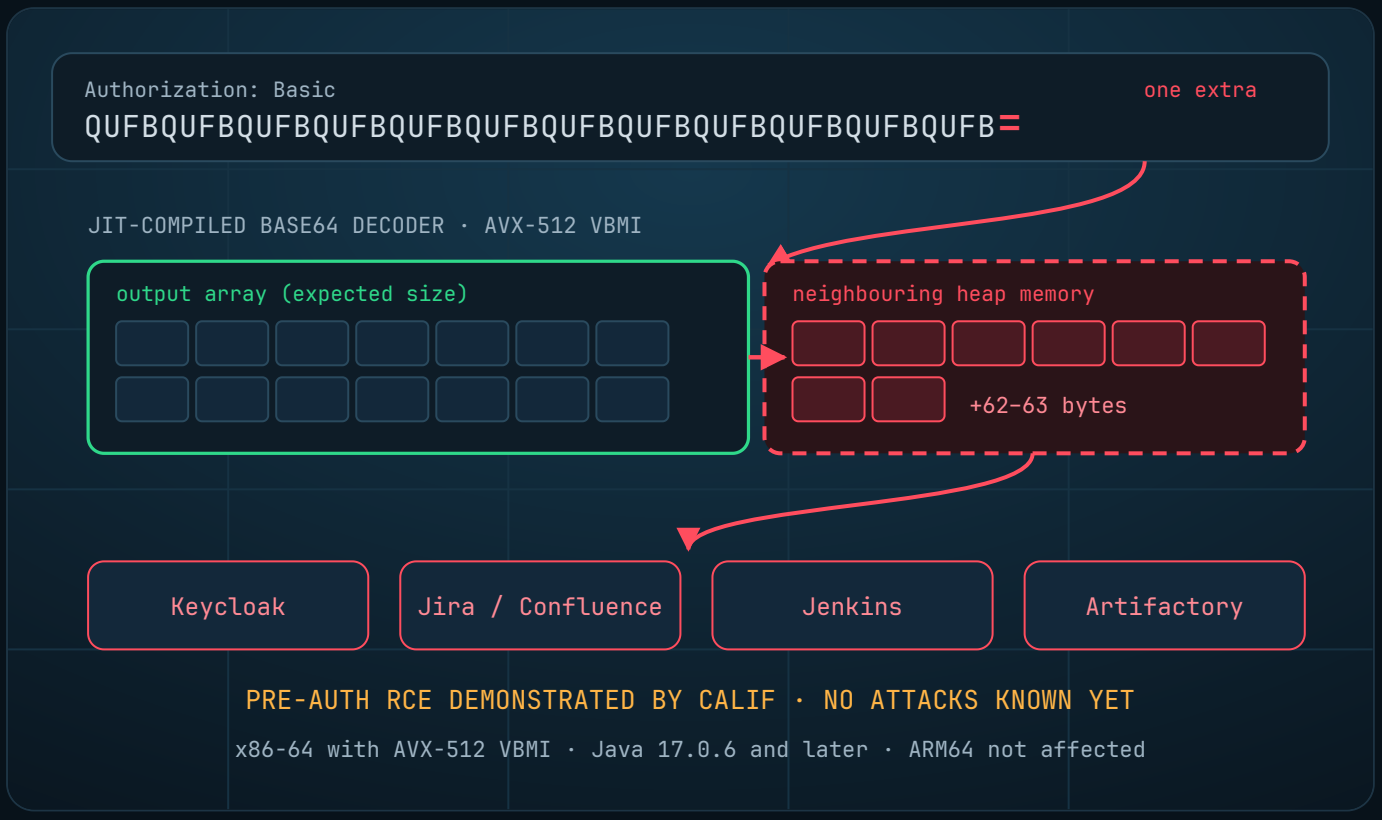
MAG212
CYBER

DAILY

Wednesday, 18 November 2026

DAILY CYBER INTELLIGENCE · CUTOFF 6:00 AM PT



JAVA4SHELL · CVE-2026-114938

One equals sign too many

A malformed Base64 string can make Java's fast decoder write past its buffer. Calif turned that into login-free code execution on Jira, Jenkins and Keycloak. Also today: a hijacked A/B-testing script on 178 websites, and Puppet's report bug is now exploited.

03 Java4Shell: one Base64 byte, pre-auth RCE
05 OPTIMJACK: a test script hit 178 brands
07 Puppet Server RCE now on CISA KEV
08 Trigram: fake recruiters, paste-a-command
09 Briefs: Ipsos, NSA outage, Telegram, INC
10 Defender's Action Desk

17 NOV
Java4Shell fix released by Oracle and OpenJDK

6 APPS
pre-auth RCE shown by Calif in default configs

178
organisations served OPTIMJACK code

1 DEC
CISA deadline for Puppet CVE-2026-115731

What matters today

Developments published or updated 16–18 November. Trigram was first published on 11 November and is included because coverage and IoC updates landed this week; Telegram follows yesterday's brief.

Java patch night

Oracle and OpenJDK fixed Java4Shell on 17 November. On x86-64 servers with AVX-512 VBMI, attacker-supplied Base64 can corrupt memory before any login check. No attacks are known yet; the attack code is withheld for now. [1][2][5]

Trusted scripts, poisoned once

For about 16 hours on 16 November, Optimizely's own CDN served a crypto clipper, card skimmer and iPhone exploit loader to visitors of 178 organisations. None of them was breached directly. [9][10]

Configuration servers under attack

CISA added Puppet Server's report-deserialization flaw to KEV with a 1 December deadline. Code execution as the Puppet user gives access to the CA signing key. [13][16]

Developers are the target

Stormshield's Trigram campaign imitates about 50 AI and blockchain brands, then asks developers to paste a command that installs an infostealer. [18][19]

THE THREE PRIORITY ACTIONS

1. **Patch Java on x86-64 servers first: internet-facing Jira, Confluence, Jenkins, Keycloak, Artifactory, PingFederate.**
   Fixed Oracle builds are 17.0.21.1, 21.0.13.1, 25.0.5.1 and 27.0.1.1. Where no fixed build exists yet, start the JVM with the Base64-intrinsic workaround and restart. [4][5]
2. **Patch or isolate Puppet and OpenVox servers today.**
   Upgrade to PE 2023.8.13, 2025.12.1 or 2026.0.1, or OpenVox Server 9.2.0 / 8.18.0. Turn off naïve autosigning and restrict who can reach the server. [13][16][26]
3. **If your site runs Optimizely Web, read every Project JavaScript field.**
   Do not just search for the payload domain: one loader variant is base64-encoded and another is inline with an eval fallback. Treat cards entered on affected checkouts as compromised. [9][10]

CONTENTS

03 Java4Shell: how one byte becomes RCE
04 Java4Shell: check, patch, verify
05 OPTIMJACK: anatomy of a script hijack
06 OPTIMJACK: what site owners do now
07 Puppet CVE-2026-115731 on KEV
08 Trigram: the paste-a-command trap
09 Briefs
10 Defender's Action Desk
11 Awareness: never paste a command
12 Sources

FIXED 17 NOV | CVSS 4.0 9.2 (CALIF) · 3.1 8.1 (ORACLE) | NO KNOWN EXPLOITATION | APP EXPLOITS WITHHELD

Java4Shell: one Base64 byte, pre-auth RCE

KEY FACT **What happened.** On 17 November Oracle and the OpenJDK project fixed CVE-2026-114938, a memory-corruption bug in Java's x86-64 Base64 decoder. Calif, which found it, says it used the bug to run code without logging in on Keycloak, Jira, Confluence, Artifactory, Jenkins and PingFederate in default configurations. [1][2][3]

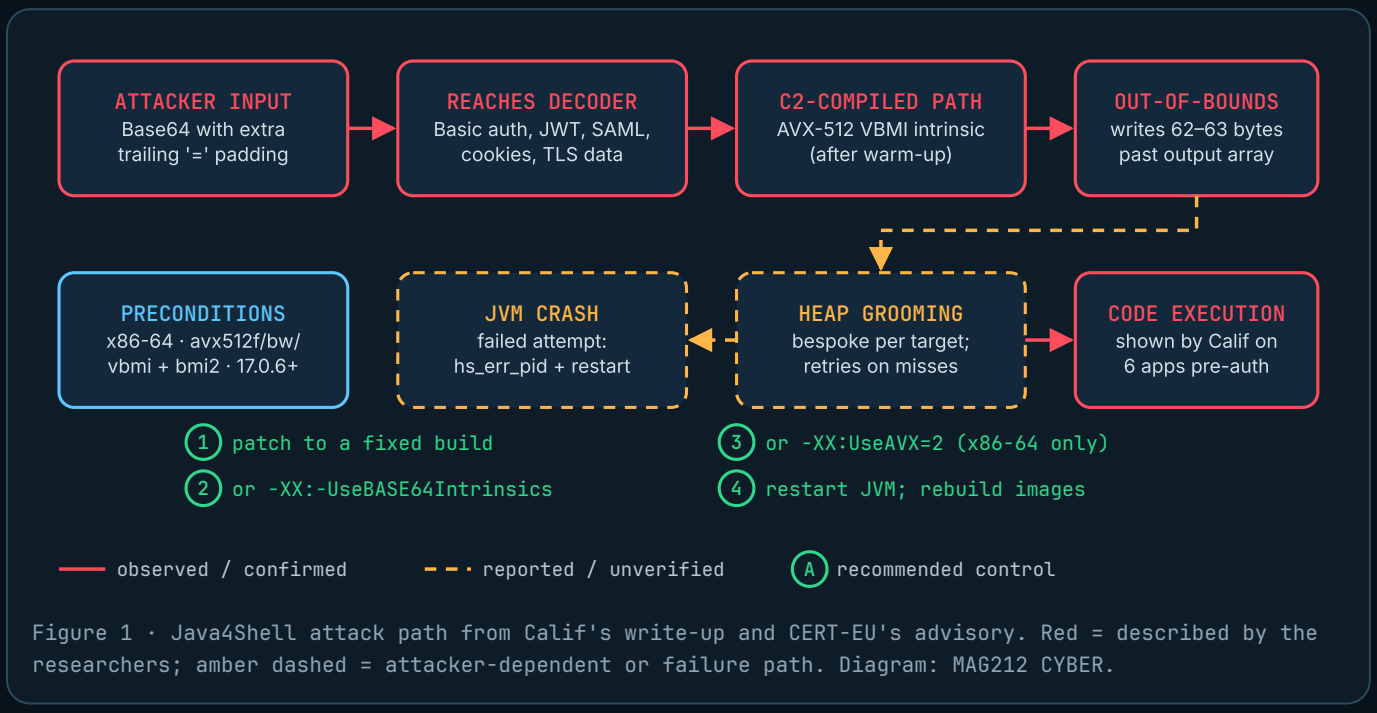


Figure 1 · Java4Shell attack path from Calif's write-up and CERT-EU's advisory. Red = described by the researchers; amber dashed = attacker-dependent or failure path. Diagram: MAG212 CYBER.

HOW THE ATTACK WORKS

Java uses a hand-tuned AVX-512 VBMI routine to decode Base64 once the method is hot enough for the C2 compiler. Given input with an unexpected trailing `=`, the routine miscalculates the output length and writes 62 or 63 bytes past the end of its array before Java rejects the input. The bytes are fixed, but the attacker can steer where they land. Any server that decodes Base64 before checking a password is reachable without one. [1][5]

Exploits are target-specific and timing-sensitive; a miss can crash the JVM, and attackers can retry. Request buffering in nginx is not a general fix. [1]

WHO IS AFFECTED

- OpenJDK 17.0.6 and later on the 17 line, plus 21, 25 and 27 before the 17 Nov fixes, in every distribution built from it. [1][4]
- Oracle Java SE 8 Performance Pack 8u511b33-perf and GraalVM for JDK 17/21. Standard Java 8 and 11 are not affected. [3][5]
- Only x86-64 CPUs with avx512f, avx512bw, avx512vbmi and bmi2: Intel Xeon Ice Lake or newer, AMD Zen 4 or newer. ARM64 is not affected. [1][4]
- Post-auth paths: Kafka, Solr, Elasticsearch, Gerrit, Spinnaker. A Java client opening TLS to a hostile server is also exposed. [1]

EXPLOITATION STATUS

Calif is withholding its application chains. Other labs reproduced crashes but not code execution, and Canada's Cyber Centre knew of no attacks. A malformed trigger input was posted publicly in an OpenJDK pull request on 9 September. [5]

Java4Shell: check, patch, verify

Products that ship their own Java need their vendor's update as well as yours. Restart services and rebuild container images after patching.

DISTRIBUTION	AFFECTED	FIXED BUILD (17 / 21 / 25 / 27)
Oracle Java SE	17.0.6–17.0.21.0.3; 21/25/27 up to .0.3	17.0.21.1 · 21.0.13.1 · 25.0.5.1 · 27.0.1.1
Oracle Java 8 Perf Pack	8u511b33-perf	8u513
Amazon Corretto	earlier builds	17.0.21.1.2 · 21.0.13.1.2 · 25.0.5.1.2 · 27.0.1.1.4
Azul Zulu	earlier builds	17.70.201 · 21.54.201 · 25.38.201 · 27.30.201
Red Hat build of OpenJDK	17.0.6 and later	not yet released when checked; see RHSB-2026-018
Temurin, Microsoft, Liberica	affected (CERT-EU)	no fixed builds listed when checked

Table 1 · Fixed builds as listed by Oracle, Amazon and Azul and compiled by The Hacker News [5]; CERT-EU [4]. Check your vendor's page before deploying.

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

CPU + JVM CHECK

```
grep -m1 '^flags' /proc/cpuinfo \
  | tr ' ' '\n' \
  | grep -E
'^(avx512f|avx512bw|avx512vbmi|bmi2)$'
java -version
java -XX:+PrintFlagsFinal -version \
  | grep UseBASE64Intrinsics
```

All four CPU flags must print for the vulnerable code to run. Then check the version of each runtime (bundled JREs too) and confirm whether the intrinsic is on. Run the last line with the same java binary and options your service uses. [4][5]

JVM startup options | service owner | CHANGES SYSTEM | NOT TESTED BY MAG212

WORKAROUND

```
-XX:+UnlockDiagnosticVMOptions
-XX:-UseBASE64Intrinsics
# or, on x86-64 hosts only:
-XX:UseAVX=2
```

Temporary workarounds until a fixed build is installed. Both need a JVM restart; UseAVX=2 can cost performance. ARM64 JVMs will not start with UseAVX=2. Do not rely on the DisableIntrinsic=_base64_decodeBlock option alone: Upwind reports Java then fails to start. Remove the flags after patching. [1][4][5]

WHAT TO LOOK FOR

- Base64 tokens of 32+ characters ending in `=` whose length is not a multiple of 4, especially in Authorization headers. [5]
- Bursts of `IllegalArgumentException` from `java.util.Base64$Decoder`. [5]
- Unexplained `hs_err_pid*.log` crash files or repeated JVM restarts. [5]
- None of these proves compromise, and their absence does not prove safety.

CONTAIN, FIX, VERIFY

1. Inventory Java on x86-64 hosts with the four CPU flags; start with internet-facing identity, CI and ticketing systems.
2. Install a fixed build, or set a workaround flag now and patch later.
3. Restart every JVM; rebuild and redeploy container images.
4. Verify: java -version shows a fixed build, or PrintFlagsFinal shows the intrinsic off.
5. If you saw crash bursts before patching, preserve logs and investigate the host.

16 NOV · ~16 HOURS | VENDOR FIXED 17 NOV | iOS EXPLOITATION UNCONFIRMED

OPTIMJACK: one test script, 178 websites

KEY FACT **What happened.** On 16 November an attacker abused a flaw in Optimizely's Web Experimentation platform to write malicious JavaScript into customers' Project JavaScript field. Optimizely's CDN then delivered it, with Optimizely's certificate, to visitors of at least 178 organisations, including the BBC, CNN, Zoom, GitLab and HSBC. None of those sites was breached directly. [9][10][11]

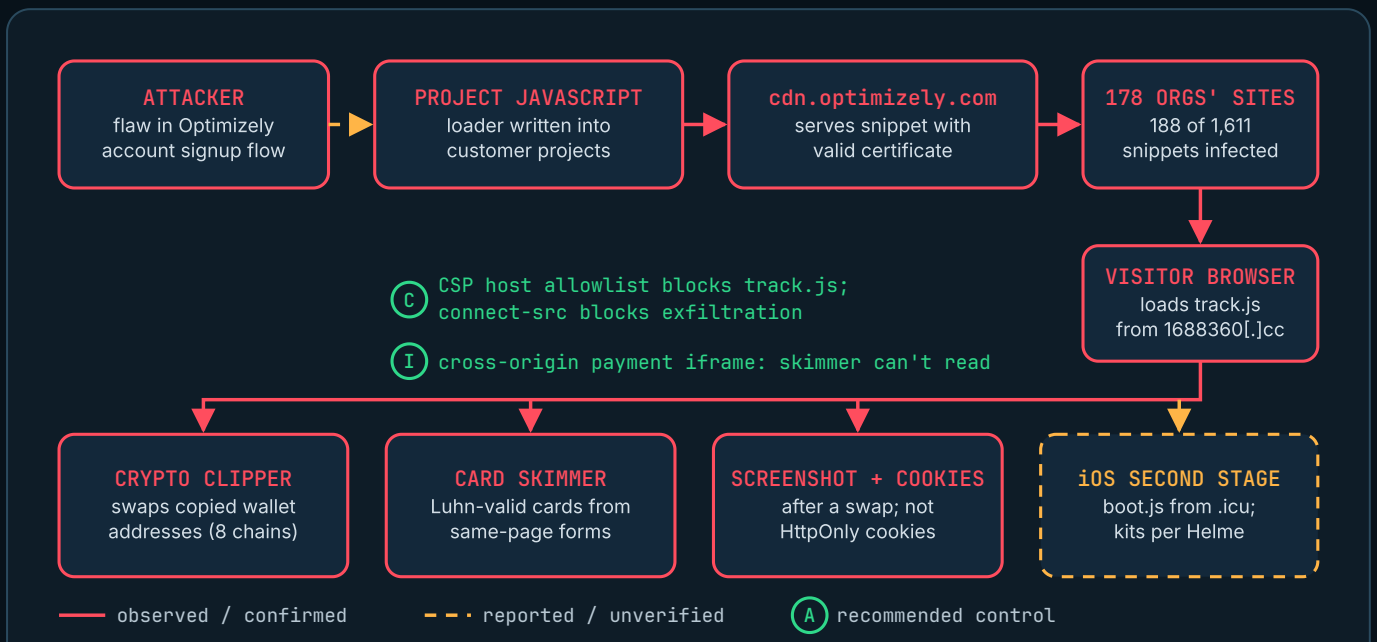


Figure 2 · OPTIMJACK delivery chain and payload, from Unit 42, StepSecurity and Report URI findings as reported. Red = observed; amber dashed = not confirmed. Diagram: MAG212 CYBER.

HOW IT WORKED

Sites load a per-project snippet from `cdn.optimizely.com/js/<project>.js`. The attacker added a loader to each project's custom code, so the CDN served exactly what the project now contained. This was not cache poisoning. Self-hosted snippets carried it too, as did Optimizely's own site and login page. [10]

Three loader variants were used: a plain script tag, a base64 URL decoded with `atob()`, and an inline copy with an `eval` fallback that survives a domain block. [10]

WHAT IT TOOK

Report URI's Scott Helme counted about $7,040 taken by 19:25 UTC on 16 November; Galaxy's Alex Thorn estimated about $2,300 sent by victims. Card losses are unknown. The skimmer could not read cross-origin payment iframes. [10]

VENDOR RESPONSE

Optimizely says it blocked the path, fixed it early on 17 November, removed the code, revoked sessions and tokens, and notified affected customers. It traced entry to its signup flow but has not explained how that gave access across projects. Equifax says it dropped Optimizely and found no compromise of its systems. [9][10][12]

TIME (UTC)	EVENT	PER
16 Nov 04:21	BBC snippet starts loading the injector from webshell[.]lol	Report URI
16 Nov 13:43	Card-skimmer block added to the payload	Report URI
16 Nov 20:40–23:11	Mass cleanup; all files clean by 23:11	Report URI
17 Nov early	Optimizely patches the flaw; payload and injector domains put on hold	Unit 42, StepSecurity

Table 2 · OPTIMJACK timeline compiled by StepSecurity [10] from Report URI data and public scans; Unit 42 [9].

OPTIMJACK: what site owners and visitors do now

The vendor removed the code. Your job is to confirm your projects are clean, decide who to notify, and stop the next third-party script from reaching checkout.

SITE OWNERS: INVESTIGATE

1. Open every Optimizely Web project and read its Project JavaScript field. Look for atob(), base64 blobs and inline code with eval.
2. Check snippets served from your own domain, not only cdn.optimizely.com.
3. Review users and API tokens in your Optimizely account; remove any you do not recognise.
4. Ask Optimizely which of your projects were changed, when, and by which account.
5. Check CSP reports and proxy logs for the payload host from 04:00 UTC 16 Nov.

SITE OWNERS: CONTAIN AND RECOVER

1. Remove injected code from the source project; a domain block alone misses the inline variant.
2. Treat card data entered on affected checkout pages during the window as compromised; follow your PCI and breach-notice process.
3. Strip marketing, testing and analytics tags from login and checkout pages.
4. Collect payments in the provider's hosted fields, in a cross-origin iframe.
5. Add a CSP host allowlist for script-src and connect-src. SRI rarely fits snippets that change with every experiment.

curl + grep (any OS) | none | READ-ONLY

NOT TESTED BY MAG212

SNIPPET CHECK

```
URL='https://cdn.optimizely.com/js/<PROJECT_ID>.js'
curl -s "$URL" \
  | grep -oE '1688360|webshell|atob\(|eval\(|\.icu' \
  | sort | uniq -c
# repeat for each self-hosted snippet URL
```

Fetches the snippet your pages load today and counts suspicious markers. A clean result now does not prove you were clean on 16 November, and legitimate experiments may use atob or eval. The source of truth is each project's Project JavaScript field and Optimizely's record of changes. [10]

INDICATORS (DEFANGED) · FROM STEPSECURITY

PAYLOAD	1688360[.]cc /track.js /hit.php /card.php /html2canvas.min.js
INJECTOR	webshell[.]lol /get.js
iOS STAGE	ios-hack[.]icu, eil786npto9u5bq[.]icu, 5vobauua3ojpklx[.]icu, l7bcsnwc7nzr3uo[.]icu and 5 more .icu hosts; paths /boot.js, /JIUJIU888/weifile.html
IPs	136[.]113[.]106[.]136 · 34[.]87[.]36[.]58 · 34[.]96[.]213[.]201
BROWSER	window._k7, _cc, _qxc, _shot; sessionStorage keys starting cc_

Full list incl. track.js hashes and wallet addresses in [10]. Domains were placed on hold 17 Nov; block them anyway and search logs from 04:00 UTC 16 Nov.

VISITORS AND CUSTOMERS

- If you paid by card on an affected site on 16 November, watch statements and consider asking for a new card.
- If you copied a crypto wallet address from an affected site, check the destination on your hardware wallet's screen before sending.
- iPhones and iPads on iOS 18.6 or earlier that visited affected sites in the window: update now; high-risk users should ask for a forensic check. Exploit pages were served; actual infections are not confirmed. [10]

CISA KEV 17 NOV · DUE 1 DEC | CVSS 4.0 9.4 | PUBLIC POC SINCE 3 NOV | RANSOMWARE USE: UNKNOWN

Puppet Server RCE is now exploited

UPDATE **What changed.** CISA added CVE-2026-115731 to its Known Exploited Vulnerabilities catalog on 17 November, giving federal agencies until 1 December. It was disclosed with fixes on 3 November, and a working exploit sits in the OpenVox advisory. [13][14][16]

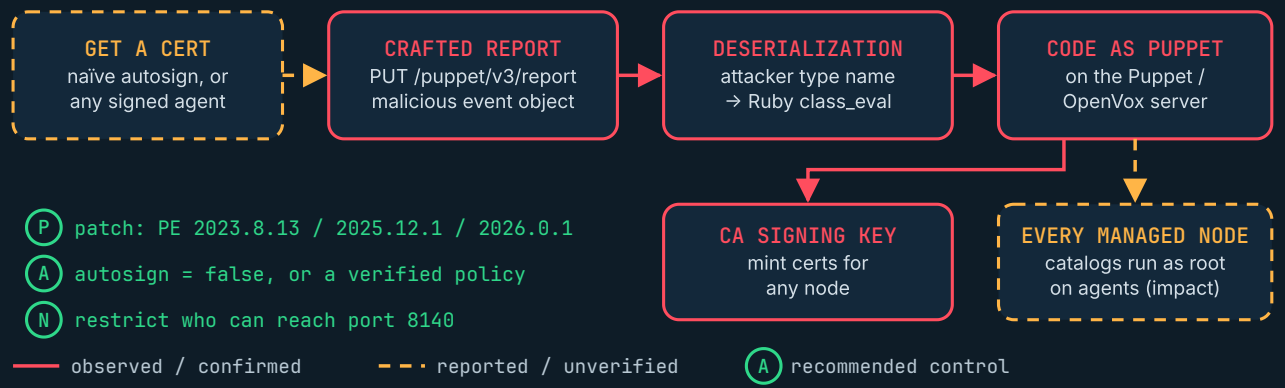


Figure 3 · CVE-2026-115731 attack path from the Perforce, OpenVox and Red Hat descriptions. Amber dashed = depends on configuration. Diagram: MAG212 CYBER.

HOW IT WORKS

After each run, agents send a JSON report to the server. An event in that report can carry a serialized Ruby object; the server trusts the attacker-supplied type name, which reaches `class_eval`. Any client holding a CA-signed agent certificate can therefore run code on the server as the Puppet service user. [14][16]

With naïve autosigning, an outsider can request a certificate and attack at once, and code execution exposes the CA signing key. Companion flaw CVE-2026-115732 (CVSS 9.0) lets a subdomain certificate impersonate its parent host; its exploitation is reported but unconfirmed. [16][17]

PRODUCT	FIXED IN
Puppet Enterprise	2023.8.13 · 2025.12.1 · 2026.0.1
Puppet Core	9.1.3 · 8.22.2
OpenVox Server / DB	9.2.0 or 8.18.0
OpenVox Agent	9.3.0 or 8.32.0
Open Source Puppet	no further updates; migrate

UNTIL YOU CAN PATCH

- Set `autosign = false` in the CA's [server] section, or use a verified policy executable. [26]
- Restrict network access to the server and to `PUT /puppet/v3/report`. [15]
- After patching, review custom auth.conf rules.

Fixed versions per [16][17].

Puppet CA server · shell | root / pe-admin | READ-ONLY | NOT TESTED BY MAG212

CA REVIEW

```
puppet config print autosign --section server
puppetserver ca list --all
```

Line 1: `true` means the CA signs every request (naïve autosigning); a path means an allowlist or policy. Line 2 lists signed and pending certificates so you can spot unknown nodes. [26][27]

STORMSHIELD CTI | ~50 BRANDS IMPERSONATED | LINKED TO UNK_DEADDROP (HIGH CONF.)

Trigram: fake jobs, a pasted command, an infostealer

KEY FACT **What Stormshield found.** An industrialised campaign impersonating about 50 AI, blockchain and tech brands targets developers in Europe and the US with fake job offers, a fake conference invitation and parcel-tracking pages. Each path ends with the victim pasting a command that installs an infostealer. Published 11 November, updated 16 November; widely reported 17 November. [18][19]

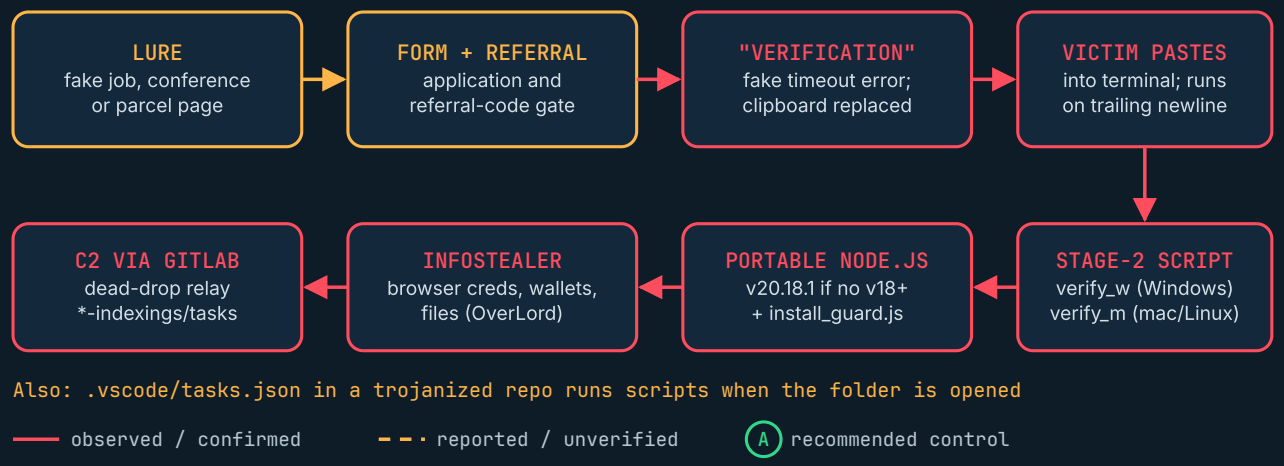


Figure 4 · Trigram infection chain from Stormshield's report. Amber = lure stages; red = malicious execution. Diagram: MAG212 CYBER.

HOW THE TRAP WORKS

After a fake application form, the page shows a ClickFix-style "verification" step. It then displays a fake error ("Operation timeout… Nonce Refreshed") and swaps the clipboard for a second command. A trailing newline makes it run the moment it is pasted. The command fetches `verify_w` or `verify_m`, which skip TLS checks, install a portable Node.js and pull `install_guard.js`. On Windows the chain uses VBScript and PowerShell and tries to strip Mark-of-the-Web; on macOS and Linux a fake password prompt appears. [18]

INFRASTRUCTURE AND ATTRIBUTION

The operators use GitHub to find targets and host trojanized repositories, a GitLab "dead drop" to publish the current C2 address, and Brevo, Resend, Mailgun and Smartlead to send mail. Stormshield links Trigram with high confidence to UNK_DeadDrop, which Proofpoint ties to the North Korean ecosystem, and notes overlaps with Kimsuky. Those are assessments, not confirmed identities. [18]

WHAT DEFENDERS LOOK FOR

- A terminal or PowerShell started from a browser, followed by a new `node` binary in a user folder.
- Outbound requests to GitLab repository paths matching `*-indexings/tasks`. [18]
- Stormshield's appendix lists about 200 IoCs and a YARA rule.

LURE	WHAT THE VICTIM SEES	WHO IT TARGETS
Recruitment	Web3, AI or tech job page stressing high pay and fully remote work; application form, then referral code	Developers, designers
Conference	Invitation to a fake "ICAGLLMBT" conference that victims are encouraged to forward to colleagues	Researchers, staff
Parcel tracking	Decoy pages imitating DHL, DPD and Aramex tracking (Stormshield [18])	Logistics and general staff

Also today

DATA BREACH · CONFIRMED INCIDENT

Ipsos investigates breach of an internal system

The market research firm says it found a cybersecurity incident affecting one internal information system, filed a complaint with authorities on 11 November and went public on 16 November. It says operations and client delivery were not affected and that it will notify clients or partners if their data is involved. It has not said what was taken, how the attacker got in, or when. [20][21]

GOVERNMENT · OUTAGE

NSA's classified network goes down; no sign of attack

NSANet, the agency's internal classified network, was degraded on Tuesday. The NSA called it "temporary degradation during scheduled routine maintenance" and said mission-critical capabilities stayed up. Two officials told CBS there was no evidence of a cyberattack; some staff were given staggered arrival times. The cause beyond maintenance is not public. [22][23]

MESSAGING · UPDATE

Telegram's new widget sandbox: two claimed bypasses

Update to yesterday's brief: Telegram moved widget JavaScript (QuickJS) into its own Android process with a seccomp filter in 13.2.2 (7303). NebuSec says two exploits run code outside it; its video shows a bot widget opening Calculator. The demo used a test server, since only approved bots can send widgets on the live service, and the filter in published source is set to audit mode. Details are withheld. [24][28]

RANSOMWARE · LAW ENFORCEMENT

Alleged INC/Lynx affiliate extradited to the US

Roman Khlynovskiy, a 43-year-old Kazakh national, was extradited from Italy. Prosecutors allege he belonged to the "8-Digits Team", an affiliate of the INC and Lynx operations that stole data from hospitals and schools in at least six US states and threatened to leak it. He faces up to 27 years in prison; the charges are allegations. [25]

ALSO NOTED

ITEM	WHY IT MATTERS	SEE
Oracle Java SE patch: 11 flaws	All remotely exploitable without auth; separate from Java4Shell	[6]
OPTIMJACK iOS stage	Coruna and DarkSword kits served; infections unconfirmed	p.06
Puppet CVE-2026-115732	Host impersonation; exploitation reported, unverified	p.07

STILL OPEN FROM EARLIER ISSUES

ITEM	STATUS ON 18 NOV	SEE
Copeland XWEB EVO: 5 flaws never to be fixed	Unchanged; isolate and replace	Daily 17 Nov
Danfoss AK-SM800A pre-auth flaws	No fix or CVE published	Daily 16 Nov
Barracuda XDR credential reset	Contacted customers should recreate credentials	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	App / platform	Find Java 17.0.6+ on x86-64 hosts with AVX-512 VBMI; patch internet-facing Jira, Confluence, Jenkins, Keycloak, Artifactory first.	p.04
TODAY	App / platform	Where no fixed build exists, add the Base64-intrinsic workaround flag and restart.	p.04
TODAY	Infrastructure	Patch Puppet Enterprise / OpenVox; set autosign = false; limit access to the server.	p.07
TODAY	Web / e-commerce	Read every Optimizely Project JavaScript field; remove injected code; review users and tokens.	p.06
48 H	SOC	Block OPTIMJACK domains; search proxy/DNS logs from 04:00 UTC 16 Nov.	p.06
48 H	SOC	Alert on Base64 decoder exception bursts and new hs_err_pid files.	p.04
48 H	Fraud / legal	Assess card exposure on affected checkouts; start notice process if needed.	p.06
THIS WEEK	Endpoint / dev	Detect terminals spawned from browsers and portable Node.js in user folders.	p.08
THIS WEEK	Web	Strip third-party tags from login and checkout; move payments to hosted iframes.	p.06
THIS MONTH	Puppet admins	Rebuild trust if compromise is suspected: the CA signing key may be exposed.	p.07

ONE-PAGE HUNT SHEET

Java	Bursts of `IllegalArgumentException` from `Base64$Decoder`; odd padding in Authorization headers.
JVM	New `hs_err_pid*.log` files; unexplained restarts on Jira, Jenkins, Keycloak.
Web	Requests to `1688360[.]cc`, `webshell[.]lol`, OPTIMJACK `.icu` hosts.
Puppet	Unknown certs in `puppetserver ca list --all`; odd report PUTs.
Endpoint	Browser → terminal → `curl`/`node`; GitLab `*-indexings/tasks`.

BEFORE YOU CLOSE A TICKET

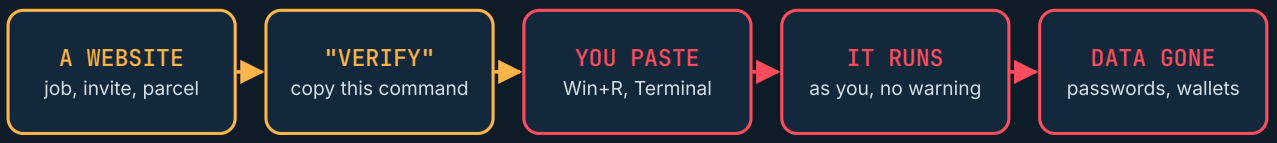
- java -version shows a fixed build on every restarted JVM.
- Container images rebuilt, not just hosts patched.
- Optimizely projects re-read after cleanup; tokens rotated.
- Puppet: patched version confirmed; autosign reviewed.

COMMAND SAFETY

Commands in this issue are read-only except the JVM workaround flags, which change startup behaviour and need a restart. All are taken from vendor documentation or the cited advisories; none was run by MAG212. Test on one system first and replace <PLACEHOLDERS> with your values.

Never paste a command a website gives you

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



No real recruiter, conference or courier asks you to paste a command.

Close the page. Report it. If you already pasted it, tell IT now: speed matters.

Trigram's page even swapped the clipboard after you copied: what you pasted was not what you saw.

Figure 5 · How paste-a-command (ClickFix) attacks work, based on the Trigram chain. Conceptual illustration, MAG212 CYBER.

FOR EVERY EMPLOYEE

- A page that says “press Win+R” or “open Terminal and paste this” to prove you are human or to finish an application is an attack.
- Copy and paste can lie: the page can change what is on your clipboard after you copy.
- Unexpected job offers with high pay, fully remote work and a “quick technical test” deserve extra suspicion.
- If you pasted something, disconnect from the network and call IT. Do not wait to see what happens.

FOR DEVELOPERS

- Open unfamiliar repos in a sandbox or disposable VM; VS Code can run .vscode/tasks.json when a folder opens.
- Never run setup scripts from a recruiter's take-home test on your work machine.
- Keep wallets, cloud keys and SSH keys off the machine you use for interviews and side projects.
- Turn on workspace trust prompts and read them.

FOR BUSINESS LEADERS

- Third-party scripts run with your brand's authority. OPTIMJACK reached 178 organisations' visitors without breaching any of them.
- Ask web teams: which outside scripts load on our login and checkout pages, and who can change them?
- Patch windows matter: Java4Shell's fix landed yesterday, and Calif plans to publish its application exploits once users have had time to upgrade. Plan the restarts now.

THREE QUESTIONS FOR YOUR NEXT TEAM MEETING

1. Would our staff recognise a fake “verification” step, and who would they call?
2. Which outside scripts can change what our customers see at checkout?
3. How fast can we restart every Java service if a patch lands tonight?

Sources

[1] Calif · 17 Nov · Java4Shell (CVE-2026-114938) technical write-up

[2] OpenJDK Vulnerability Group · 17 Nov · OpenJDK vulnerability advisory 2026-11-17

[3] Oracle · 17 Nov · Critical Security Patch Update, November 2026

[4] CERT-EU · 17 Nov · Security Advisory 2026-021: Java SE and OpenJDK (PDF)

[5] The Hacker News · 17 Nov · Java4Shell enables pre-auth RCE in Jira, Jenkins, Keycloak and more

[6] The Hacker News · 17 Nov · Oracle to patch 11 Java flaws as critical OpenJDK RCE report emerges

[7] Red Hat · 17 Nov · Security bulletin RHSB-2026-018 (Java4Shell)

[8] SentinelOne · 17 Nov · Defending against Java4Shell on AVX-512 CPUs

[9] Palo Alto Networks Unit 42 · 17 Nov · Borrowed code, real consequences: what OPTIMJACK teaches us

[10] StepSecurity · 17 Nov · OPTIMJACK: Optimizely-hosted scripts loaded a crypto clipper and card skimmer

[11] Security Affairs · 17 Nov · OPTIMJACK: BBC, CNN and Zoom among targets of Optimizely script hijacking

[12] Cybernews · 17 Nov · Zoom, IKEA, HSBC among 178 websites infected with hidden malware

[13] CISA · 17 Nov · CISA adds one known exploited vulnerability to catalog

[14] Perforce · 3 Nov · CVE-2026-115731: report deserialization code execution

[15] Red Hat · Nov · CVE-2026-115731 description and mitigation

[16] SecurityOnline · Nov · Puppet Server RCE CVE-2026-115731: public PoC

[17] SecurityWeek · 17 Nov · Critical Perforce Puppet RCE exploited in attacks

[18] Stormshield · 11 Nov, upd. 16 Nov · Trigram campaign: AI, blockchain and logistics (CTI report)

[19] The Hacker News · 17 Nov · Trigram campaign impersonates about 50 AI and blockchain brands

[20] Ipsos · 16 Nov · Ipsos filed a complaint regarding a breach on one of its internal systems

[21] SecurityWeek · 17 Nov · Market research giant Ipsos investigating breach of internal system

[22] Associated Press (via WRAL) · 17 Nov · Classified communications network at the NSA goes down, official says

[23] CBS News · 17 Nov · NSA's classified internal network goes down, sources say

[24] The Hacker News · 17 Nov · Researchers claim two RCE exploits that bypass Telegram's new Android defenses

[25] BleepingComputer · 17 Nov · Ransomware affiliate suspect extradited to US, faces 27 years in prison

[26] Puppet documentation · Docs · Autosigning certificate requests

[27] Ubuntu manpages · Docs · puppetserver-ca(1): Puppet Server CA management command

[28] MAG212 CYBER · 17 Nov · Daily 17 Nov: Telegram widgets RCE dispute and other briefs

HOW WE VERIFIED THIS ISSUE

- Primary sources read: Calif's Java4Shell write-up, CERT-EU's advisory, Oracle's November patch update, Unit 42's OPTIMJACK post, Stormshield's Trigram report, CISA's KEV alert, Ipsos's press release.
- The OpenJDK advisory page and SecurityWeek's Puppet article did not load for us; Java fixed builds come from Oracle, CERT-EU and The Hacker News's table, and Puppet fixed versions from SecurityOnline and SecurityWeek's summary as indexed. Check vendor pages before deploying.
- OPTIMJACK timings, payload behaviour and IoCs come from StepSecurity's analysis citing Report URI; Optimizely's statement is as reported there and by Unit 42. iOS infections are not confirmed.
- 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 · 18 November 2026
Understand the threat. Build the defense.