TECHNICAL BRIEF

Prepared Nov 27, 2026, 5:31 PM PST

CloudLinux: CVE-2026-123007 NGINX2Root: unauthenticated HTTP/2 remote code execution in nginx

Status: Ongoing

Started Nov 18, 2026, 12:00 PM PST · CloudLinux's estimate: nginx fixes out now; CloudLinux 9.9 reaches 9.8 servers in batches over about two weeks from November 16; kernel SCTP fix: no CloudLinux date published

WHERE THINGS STAND

CloudLinux's nginx2root advisory is unchanged since its November 19 update: fixed nginx builds are out, but CloudLinux 9.8 servers on nginx 1.26 get the fix only through the 9.9 rollout or its bypass repository. The Linux kernel SCTP flaw used for the root step still has no CloudLinux kernel build, and exploitation reports remain disputed. A news report says an upstream kernel fix landed on November 22, but that is unconfirmed.

Affected: CloudLinux 7 (ELS), 8, 9 and 10 system nginx, CloudLinux 9.8 with system nginx 1.26, cPanel ea-nginx, Imunify360 WebShield bundle nginx, nginx 1.9.5 through 1.31.8 (upstream, CVE-2026-123007), nginx 1.21.4 through 1.31.9 (upstream, CVE-2026-132779)

REFERENCE NUMBERS

ID	TYPE	SEVERITY	EXPLOITED	LINK
CVE-2026-123007	CVE	CVSS 9.2 · critical	No	https://www.cve.org/CVERecord?id=CVE-2026-123007
CVE-2026-123633	CVE	CVSS 9.2 · critical	No	https://nvd.nist.gov/vuln/detail/cve-2026-123633
CVE-2026-123634	CVE	CVSS 9.2 · critical	No	https://my.f5.com/manage/s/article/K000163925
CVE-2026-121810	CVE	CVSS 9.2 · critical	No	https://my.f5.com/manage/s/article/K000163927
CVE-2026-113425	CVE	CVSS 9.2 · critical	No	https://my.f5.com/manage/s/article/K000163931
CVE-2026-132779	CVE	CVSS 5.3 · medium	No	https://nginx.org/en/security_advisories.html
K000163926	vendor	CVSS 9.2 · critical	No	https://my.f5.com/manage/s/article/K000163926

AFFECTED VERSIONS AND FIXES

Every publicly affected version line found. Rows marked (BIS) are systems BIS runs.

PRODUCT / DISTRIBUTION	AFFECTED	FIXED IN	STATUS	SOURCE
(BIS) Linux kernel SCTP send path (no CVE)	CloudLinux 9.8 kernel 5.14 not confirmed	—	**NO FIX YET**	MyCERT advisory MA-1512.112026, 2026-11-21
(BIS) CloudLinux 9.8 system nginx 1.26	before nginx-1.26.3-10.module_el9.9.0+357+ccfac862.1.alma.2 (CloudLinux 9.9)	nginx-1.26.3-10.module_el9.9.0+357+ccfac862.1.alma.2 (on CloudLinux 9.9)	**WAITING**	CloudLinux security advisory (re-read Nov 28; 9.9 rolling out in batches), 2026-11-19
(BIS) Linux kernel SCTP send path (no CVE)	Linux 4.15 and later; CloudLinux 9.8 kernel 5.14 not confirmed	—	**UNCONFIRMED**	BreachNews (report of upstream Linux 7.4-rc4 fix Nov 22; unconfirmed; no CloudLinux build), 2026-11-25

Questions? Contact BIS Computer Solutions, Inc.

Phone: +1-818-248-5023 · Fax: +1-818-249-1169 · Email: support@biscomputer.com · Web: www.biscomputer.com

(BIS) CloudLinux 9 system nginx 1.20 (default)	before nginx-1.20.1-32.el9_9.1.cloudlinux.3	nginx-1.20.1-32.el9_9.1.cloudlinux.3	**FIXED**	CloudLinux security advisory (last updated 2026-11-19; re-read Nov 28), 2026-11-19
(BIS) CloudLinux 9 system nginx 1.22	before nginx-1.22.1-8.module_el9.9.0+439+b175c265.1.cloudlinux.4	nginx-1.22.1-8.module_el9.9.0+439+b175c265.1.cloudlinux.4	**FIXED**	CloudLinux security advisory (re-read Nov 28), 2026-11-19
(BIS) CloudLinux 9 system nginx 1.24	before nginx-1.24.0-9.module_el9.9.0+440+16ab46e3.1.cloudlinux.3	nginx-1.24.0-9.module_el9.9.0+440+16ab46e3.1.cloudlinux.3	**FIXED**	CloudLinux security advisory (re-read Nov 28), 2026-11-19
(BIS) CloudLinux 8 system nginx 1.20 / 1.22 / 1.24	before the fixed builds listed in the advisory	nginx-1.20.1-1.module_el8.10.0+7346+9bd89172.1.cloudlinux.3; nginx-1.22.1-1.module_el8.10.0+7347+6d9c8a63.1.cloudlinux.3; nginx-1.24.0-3.module_el8.10.0+7348+69171071.6.cloudlinux.3	**FIXED**	CloudLinux security advisory (re-read Nov 28), 2026-11-19
(BIS) CloudLinux 8 system nginx 1.14 / 1.16 / 1.18	before the fixed builds in CloudLinux's support article	nginx-1.14.1-9.module_el8.10.0+7343+af250afe.cloudlinux.4 (1.14; 1.16 and 1.18 listed in article)	**FIXED**	CloudLinux support article (undated; covers CVE-2026-123007 and CVE-2026-123633 only)
CloudLinux 7 ELS system nginx 1.20	before the fixed build in CloudLinux's advisory	fixed build listed in CloudLinux advisory	**FIXED**	CloudLinux security advisory (re-read Nov 28), 2026-11-19
cPanel ea-nginx	before ea-nginx-1.31.9-1~urgent	ea-nginx-1.31.9-1~urgent	**FIXED**	CloudLinux security advisory (re-read Nov 28), 2026-11-18
Imunify360 WebShield bundle (nginx inside)	before 1.50.1-3	1.50.1-3 (1.50.3 or later on beta channel; 1.50.2-1 not fixed)	**FIXED**	Imunify360 blog (undated)

WORKAROUNDS UNTIL A FIX IS INSTALLED

- Turn HTTP/2 off in every server block on the listening port (nginx 1.25.1 and later: http2 off;)
- Keep HTTP/3 off on CloudLinux 9.8 nginx 1.26 servers until 9.9 arrives
- Turning HTTP/2 off blocks CVE-2026-123007 and CVE-2026-123633 only; the other flaws need their own updates
- Block the sctp module on hosts that do not use SCTP (install sctp /bin/false); this does not unload a loaded module

HOW TO CHECK IF A SYSTEM IS AFFECTED

```
rpm -q nginx ea-nginx
grep -rn 'http2' /etc/nginx/
lsmod | grep sctp; modprobe -n -v sctp
uname -r (staff-supplied kernel 5.14.0-611.55.1.el9_7.x86_64 is not named in CloudLinux's advisory; unverified)
```

ROOT CAUSE

Nginx HTTP/2 flow-control integer overflow and use-after-free flaws allow worker code execution; a Linux kernel SCTP send-path use-after-free (no CVE, no CloudLinux fix) can lift a worker foothold to root.

EXPLOITATION

Singapore's CSA reports CVE-2026-123007 is reportedly being actively exploited, with a public PoC. StepSecurity (24 Nov), CERT-EU and Sophos (23 Nov) report no confirmed exploitation; CISA's KEV catalog does not list these CVEs (BreachNews, Nov 25). CrowdStrike reports a public PoC but no confirmed exploitation; Qualys reports the researchers claim a working exploit over public clouds (unconfirmed). The sources conflict.

WHAT THE IT COMMUNITY IS SAYING

Only one post in the last seven days is clearly on this topic: a repost on X (about 4 days old) saying Palo Alto Networks confirmed the HTTP/2 nginx flaws affect PAN-OS and Panorama, with workarounds. Nearly all the other discussion I found is from November 18–19, outside the window, and none of the in-window posts report breakage, a working fix, or a CloudLinux-specific update.

From public posts by IT administrators; not confirmed by the vendor.

TIMELINE (NEWEST FIRST)

Nov 27, 2026, 5:31 PM PST

New: the Imunify360 WebShield bundle has a fixed build (1.50.1-3) on CloudLinux's own blog; the CloudLinux nginx2root advisory is unchanged and still has no kernel fix.

Nov 27, 2026, 5:29 PM PST

CloudLinux's November 19 advisory lists fixed nginx packages for CloudLinux OS 9, and public exploit reports are now on record.

Nov 27, 2026, 4:05 PM PST

New: a news report says an upstream Linux kernel fix for the SCTP flaw landed on November 22; it is unconfirmed, and CloudLinux's advisory still shows no kernel build.

Nov 27, 2026, 12:03 PM PST

One new item: a CloudLinux support article says servers that took the November 18 nginx update should run the update again; the advisory itself could not be re-read this run.

Nov 27, 2026, 8:01 AM PST

One new third-party claim: the NGINX2Root researchers say their own exploit works over public clouds, unconfirmed by any vendor. CloudLinux's advisory could not be re-read this run, so its status is carried forward.

Nov 26, 2026, 3:53 PM PST

Two small new items: a StepSecurity report (24 Nov) that no exploitation has been seen, which conflicts with the Singapore CSA claim, and a possible CSA alert-number mismatch; CloudLinux's own pages could not be re-read this run.

Nov 26, 2026, 3:47 AM PST

Singapore's CSA says CVE-2026-123007 is reportedly being actively exploited, which no vendor has confirmed; CloudLinux's advisory is unchanged, with no new nginx or kernel build.

Nov 25, 2026, 4:00 PM PST

Singapore CSA reports CVE-2026-123007 reportedly exploited (unconfirmed by vendors) (CSA Singapore)

Nov 25, 2026, 11:38 AM PST

New: nginx 1.30.8 and 1.31.10 were released on November 23, 2026 to fix a separate medium-severity nginx flaw, CVE-2026-132779; the CloudLinux pages could not be re-read this run, so their status is carried from the last check.

Nov 24, 2026, 7:31 PM PST

New: CloudLinux's nginx2root advisory adds an HTTP/3 turn-off step for 9.8 servers on nginx 1.26 and names a bypass repository that needs checking; the kernel SCTP fix is still unpublished.

Nov 24, 2026, 3:29 PM PST

New since the last check: MyCERT (Nov 21) confirms the Linux SCTP kernel flaw is still unpatched, and CrowdStrike reports a public proof-of-concept; CloudLinux's advisory is unchanged.

Nov 23, 2026, 4:00 PM PST

StepSecurity reports no exploitation seen; conflicts with CSA report (StepSecurity)

Nov 23, 2026, 7:39 AM PST

nginx 1.30.8 and 1.31.10 released (CVE-2026-132779 fix) (nginx.org)

Nov 21, 2026, 4:00 PM PST

Upstream Linux 7.4-rc4 reportedly carries SCTP fix (unconfirmed) (BreachNews)

Nov 20, 2026, 4:00 PM PST

MyCERT says SCTP kernel flaw still unpatched, no CVE (MyCERT)

Nov 19, 2026, 5:50 AM PST

CloudLinux publishes fixed builds; CL9 nginx 1.26 waits for 9.9 (CloudLinux)

Nov 17, 2026, 9:00 PM PST

nginx 1.30.7 and 1.31.9 released with fixes (nginx.org)

Nov 16, 2026, 8:09 AM PST

CloudLinux 9.9 stable released; 9.8 upgrade rolls out in batches (CloudLinux)

SOURCES

Imunify360 blog — https://blog.imunify360.com/nginx2root-cve-2026-123007-imunify360-webshield/