

Alert Bulletin

Bulletin N.: 116

Publication Date: 19/10/2026

Subject: Alert 2026-116 Critical vulnerabilities in NGINX allow DoS service and RCE.

Traffic Light Protocol (TLP): White

Affected product(s):

NGINX Open Source

CVE	Affected versions according to nginx.org	Fixed versions
CVE-2026-15176	0.1.29 to 1.31.6, except branches that already include the fix	1.30.6 in the stable branch or 1.31.7 in the main branch, and later
CVE-2026-93479	1.30.0 to 1.30.5 and 1.31.2 to 1.31.6	1.30.6 or 1.31.7, and later
CVE-2026-97205	0.8.11 to 1.31.6, except branches that already include the fix	1.30.6 in the stable branch or 1.31.7 in the main branch, and later

NGINX Plus and integrated products

Product	Affected versions or scope	Fix released
NGINX Plus 37.x	37.0.0 to 37.0.4, for the three CVEs	37.0.5.1 or 37.1.0.1.
NGINX Plus R33-R36	The branches are listed as affected in the advisories	No fix listed in those branches; consult the supported upgrade path.
F5 WAF for NGINX	Affected versions within the 5.9.0–5.15.0 range; details vary by CVE	5.14.2 or 5.16.0, depending on the applicable branch.
F5 DoS for NGINX	4.8.0 to 4.10.0	4.11.0.
NGINX Gateway Fabric	The impact depends on the branch and the CVE; advisories include 2.1.0–2.7.2	2.8.0 for the indicated 2.x branch.
NGINX Ingress Controller	For CVE-2026-97205: 5.6.0 to 5.6.3	5.7.0. Validate the other CVEs separately.
NGINX Instance Manager	For CVE-2026-97205: 2.18.0 to 2.23.0	2.24.0. Validate the other CVEs separately.

Description

Three memory corruption vulnerabilities were disclosed in NGINX: **CVE-2026-15176**, related to the use of *alias* and *rewrite*; **CVE-2026-93479**, associated with the evaluation of variables and regular expression captures; and **CVE-2026-97205**, linked to the combined use of SSI and asynchronous I/O operations —AIO—. All three have a CVSS v4.0 score of 9.2 and may allow unauthenticated remote attackers to cause worker processes to crash. Code execution is possible under additional conditions, such as ASLR being disabled or that protection being bypassed. Exposure depends on specific configurations, not merely on the presence of NGINX.

Vulnerabilities and exposure conditions:

CVE	Description	Configuration the administrator should review
CVE-2026-15176	Buffer overflow in a worker process when converting a modified URI to a file path.	Use of alias in a location block, when rewrite modifies the URI and it is subsequently mapped to a path; also review the use of \$request_filename.
CVE-2026-93479	Buffer overflow when evaluating text expressions with variables, impacting document root calculation and request logging.	map directives with regular expressions whose capture variables are used in root or in the access log format before referencing the map's output variable.
CVE-2026-97205	Use-after-free under certain configurations.	Combined use of AIO and SSI pages with include virtual instructions.

Solution

The solution is to update NGINX Open Source to 1.30.6 or 1.31.7, or later in the corresponding branch, and install the fixed versions that F5 indicates for NGINX Plus and the products that integrate it.

Priority should be given to servers exposed to the Internet that use the vulnerable configurations; verify the version actually running after the change and complete the substitution of old processes or containers.

Additional information:

- F5 — CVE-2026-15176:
<https://my.f5.com/manage/s/article/K000162416f5>
- F5 — CVE-2026-93479:
<https://my.f5.com/manage/s/article/K000162607f5>
- F5 — CVE-2026-97205:
<https://my.f5.com/manage/s/article/K000162608f5>
- NGINX — official security advisories:
https://nginx.org/en/security_advisories.html
- BleepingComputer:
<https://www.bleepingcomputer.com/news/security/f5-releases-out-of-band-patches-for-critical-nginx-vulnerabilities/>