GOVERNMENT OF THE REPUBLIC OF VANUATU

PRIME MINISTER'S OFFICE

CERTVU
DEPARTMENT OF COMMUNICATIONS & DIGITAL TRANSFORMATION

PM B 9108 Port Vila, Vanuatu

Tel: (678) 33380

GOUVERNEMENT DE LA REPUBLIQUE DU VANUATU

BUREAU DU PREMIER MINISTRE

CERTVU

DEPARTMENT DE COMMUNICATION ET DE TRANSFORMATION NUMERIQUE

SPP 9108 Port Vila, Vanuatu
Tel: (678) 33380

19 November 2026

Advisory 387: NGINX HTTP/2, HTTP/3, DNS Resolver, and Mail Proxy Multiple Critical Remote Code Execution Vulnerabilities ("NGINX2Root") (CVE-2026-123007, CVE-2026-123633, CVE-2026-123634, CVE-2026-121810, and CVE-2026-113425).

Release Date: 18th November 2026
Impact: CRITICAL
TLP: CLEAR

The Department of Communications and Digital Transformation (DCDT) through CERT Vanuatu (CERTVU), provides the following advisory.

This alert is relevant to Organizations and System/Network administrators that operate NGINX Open Source, NGINX Plus, or products built on NGINX (including Kubernetes ingress-nginx and Linux distribution packages) as a web server, reverse proxy, or load balancer. This alert is intended to be understood by technical users and systems administrators.

What is it?

On 18 November 2026, F5 released NGINX Open Source 1.30.7/1.31.9 and updated NGINX Plus builds fixing five critical memory-corruption vulnerabilities, being CVE-2026-123007, CVE-2026-123633, CVE-2026-123634, CVE-2026-121810, and CVE-2026-113425. Collectively dubbed "NGINX2Root" by researchers. NGINX is one of the world's most widely deployed web servers, reverse proxies, and load balancers, underpinning a large share of internet-facing infrastructure globally. Each vulnerability can allow an unauthenticated remote attacker to execute code with the privileges of the NGINX worker process, under a different server configuration (HTTP/2, HTTP/3, a DNS-resolving proxy configuration, or the mail proxy).

- CVE-2026-123007 (HTTP/2 enabled; affects every release 1.9.5 through 1.31.8; CVSS 4.0 9.2 Critical): an integer underflow in HTTP/2 flow control leads to an out-of-bounds memory copy that can disclose memory and corrupt the heap, including on servers that only serve static content.

- CVE-2026-123633 (HTTP/2 enabled, with requests forwarded to a backend server; affects 1.19.7 through 1.31.8; CVSS 4.0 9.2 Critical): a use-after-free in HTTP/2 connection handling, triggered when an idle connection is closed and freed while a forwarded request still uses it.
- CVE-2026-123634 (DNS resolution during request processing, such as proxy_pass with variables, combined with subrequests such as mirror; affects 0.6.18 through 1.31.8; CVSS 4.0 9.2 Critical): a use-after-free in the DNS resolver during response processing.
- CVE-2026-121810 (HTTP/3 / QUIC enabled, with requests forwarded to a backend server; affects 1.25.0 through 1.31.8; CVSS 4.0 9.2 Critical): a use-after-free in HTTP/3 request handling.
- CVE-2026-113425 (Mail proxy using proxy on and auth_http; affects 0.5.33 through 1.31.8; CVSS 4.0 9.2 Critical): a use-after-free in the mail proxy module.

What are the systems affected?

The vulnerabilities affect:

- NGINX Open Source (stable), versions 1.9.5 through 1.30.6
- NGINX Open Source (mainline), versions 1.31.0 through 1.31.8
- NGINX Plus 37.x, versions 37.0.0 through 37.0.7.1 and 37.1.0 through 37.2.0.1
- NGINX Plus R-series, R34 through R36, all builds
- Linux distribution packages containing an affected packaged NGINX version
- Kubernetes ingress-nginx releases bundling an affected NGINX version
- Products that bundle NGINX (vendor-specific)

What does this mean?

Successful exploitation may allow attackers to:

- Execute arbitrary code with the privileges of the NGINX worker process, without authentication, by sending crafted HTTP/2, HTTP/3, DNS-triggering, or mail-proxy traffic.
- Disclose process memory and corrupt the heap, potentially exposing sensitive data the server handles.
- Crash NGINX worker processes, causing denial of service, even where full code execution is not achieved.
- Chain CVE-2026-123007 with an unpatched Linux kernel SCTP vulnerability to achieve full host compromise, including escape from a Docker container to the underlying host, as researchers have already demonstrated.

Mitigation process

CERTVU recommends the following:

1. Apply the vendor fix without delay
Upgrade to NGINX Open Source 1.30.7 or 1.31.9, or NGINX Plus 37.0.8.1 or 37.3.0.1

2. Disable HTTP/2 where updates cannot be applied immediately
On NGINX 1.25.1 and later.

3. Disable HTTP/3 (CVE-2026-121810)
4. Remove request-time DNS lookups (CVE-2026-123634)
5. Restrict the mail proxy (CVE-2026-113425)
6. Block the SCTP kernel module
7. Migrate from Kubernetes ingress-nginx

Report any suspected compromise involving NGINX to CERTVU at incident@cert.gov.vu or on telephone (678) 33380.

Reference

1. https://nginx.org/en/security_advisories.html
2. https://www.cve.org/CVERecord?id=CVE-2026-123007
3. https://www.cve.org/CVERecord?id=CVE-2026-123633
4. https://www.cve.org/CVERecord?id=CVE-2026-123634
5. https://www.cve.org/CVERecord?id=CVE-2026-121810
6. https://www.cve.org/CVERecord?id=CVE-2026-113425