مجلس الأمن السيبراني
CYBER SECURITY COUNCIL
United Arab Emirates

Critical NGINX Zero-Day “nginx-poolslip” Enables Remote Code Execution

Tracking #:432319009

Date:21-05-2026

TLP: WHITE

EXECUTIVE SUMMARY:

The UAE Cyber Security Council has observed that a newly disclosed zero-day vulnerability, dubbed "nginx-poolslip," has been identified in NGINX version 1.31.0. The flaw reportedly allows unauthenticated remote code execution (RCE) through weaknesses in NGINX's internal memory pool management mechanism.

TECHNICAL DETAILS:

A newly disclosed zero-day vulnerability, dubbed "nginx-poolslip," has been identified in NGINX version 1.31.0. The flaw reportedly allows unauthenticated remote code execution (RCE) through weaknesses in NGINX's internal memory pool management mechanism.
The vulnerability was discovered by security researcher Vega of the NebSec research team and publicly disclosed on May 21, 2026. According to available reports, successful exploitation could enable attackers to bypass Address Space Layout Randomization (ASLR) protections and execute arbitrary code on vulnerable servers.

At the time of publication:

- No official CVE identifier has been assigned
- No vendor patch has been released
- Public proof-of-concept (PoC) exploit code has not been released
- The issue is considered highly critical due to NGINX's widespread deployment across internet-facing infrastructure

Organizations using NGINX for web hosting, reverse proxying, load balancing, or API gateway functions should immediately implement defensive mitigations and closely monitor vendor advisories.

The vulnerability reportedly exists within NGINX's internal memory pool management subsystem, which is responsible for allocation and handling of request-related memory objects.
Researchers indicate that attackers may exploit memory corruption conditions to:

- Trigger unsafe memory operations
- Manipulate heap structures
- Bypass ASLR protections
- Execute arbitrary malicious payloads remotely

The flaw is especially concerning because:

- It affects the latest stable release
- It may bypass mitigations introduced for previous NGINX vulnerabilities
- It targets internet-facing infrastructure commonly exposed to untrusted traffic

According to researchers, the issue may also be connected to residual attack surface left behind after the remediation of:

- CVE-2026-42945 — a critical heap buffer overflow vulnerability in ngx_http_rewrite_module

That earlier vulnerability reportedly existed in the codebase for over 18 years and exposed millions of servers to denial-of-service and potential RCE risks.
NebSec researchers claim that although fixes were introduced in versions 1.31.0 and 1.30.1, the underlying memory handling exposure was not fully eliminated.

RECOMMENDATIONS:

- Monitor NebSec and F5 security advisories for updates, detection guidance, and patch releases
- Restrict exposure of NGINX administrative and management interfaces to minimize the external attack surface
- Deploy Web Application Firewall (WAF) protections to detect and block malicious or malformed HTTP requests
- Ensure Linux ASLR protections are fully enabled (randomize_va_space=2) across all affected systems
- Review and audit NGINX configurations using rewrite, if, and set directives, especially those relying on unnamed PCRE capture groups
- Reduce unnecessary module exposure and disable unused NGINX functionality where possible
- Increase monitoring for worker crashes, segmentation faults, or abnormal memory behavior that may indicate exploitation attempts
- Implement network segmentation and least-privilege controls for internet-facing NGINX instances
- Prepare emergency patch deployment procedures to rapidly apply vendor fixes once released

Kindly circulate this information to your subsidiaries and partners as well as share with us any relevant information and findings.

The UAE Cyber Security Council extends its appreciation for the continued collaboration.

REFERENCES:

- https://nebusec.ai/research/