

NGINX Patches Five Vulnerabilities Including Potential Remote Code Execution and TLS Session Forgery



NGINX released versions 1.30.6 and 1.31.7 on October 14 to address five vulnerabilities, including three memory flaws that may enable remote code execution and a TLS bug allowing session forgery.

- NGINX versions 1.30.6 and 1.31.7 released October 14, 2025 to fix five security vulnerabilities
- Three memory-related flaws could crash worker processes or potentially allow remote code execution under specific configurations
- A TLS vulnerability permits attackers to forge sessions, potentially bypassing client certificate verification
- One vulnerability has existed in every NGINX release since May 2005
- All three memory bugs require specific server configurations to be exploitable

Vulnerability Overview

F5, the company behind NGINX, released two updated versions on October 14, 2025 to remediate five security vulnerabilities affecting the widely deployed web server and reverse proxy software. NGINX versions 1.30.6 and 1.31.7 address three memory-related flaws that could crash worker processes or, under certain conditions, potentially allow an attacker to execute arbitrary code. Each of these memory bugs requires a specific server configuration to be exploitable.

A fourth vulnerability affects **TLS session handling** and permits an attacker to forge a session, which may allow bypassing client certificate verification controls. Notably, one of the patched flaws has been present in every NGINX release since May 2005, representing a nearly two-decade exposure window.

Risk to Regulated Institutions

NGINX is commonly deployed in front-end web infrastructure, API gateways, and load-balancing tiers across financial services, healthcare, and government sectors in the Kingdom. The potential for remote code execution, even when configuration-dependent, represents a material risk to confidentiality, integrity, and availability of critical services. The TLS session forgery vulnerability is particularly concerning for institutions relying on mutual TLS authentication to enforce access controls for sensitive applications or APIs.

Immediate Response

Organizations should inventory all NGINX deployments, prioritize internet-facing and business-critical instances, and schedule patching to the latest stable releases. Configuration reviews should confirm whether specific settings that enable exploitation of the memory flaws are in use, and TLS client certificate authentication mechanisms should be validated.

What to do now

1. Inventory all NGINX deployments across production, staging, and development environments
2. Prioritize patching of internet-facing NGINX instances and those handling sensitive data or authentication
3. Upgrade to NGINX version 1.30.6 or 1.31.7 following change management procedures
4. Review NGINX configurations to identify settings that may enable exploitation of the memory vulnerabilities
5. Validate TLS client certificate authentication mechanisms and access control policies
6. Monitor NGINX error logs and security event logs for anomalous worker process crashes or authentication bypasses