

F5 Issues Emergency Patches for Critical NGINX Code Execution Flaws



F5 has released out-of-band patches for three critical NGINX vulnerabilities enabling remote code execution and denial-of-service attacks on systems with non-default configurations.

- Three critical vulnerabilities (CVE-2026-15176, CVE-2026-97205, CVE-2026-93479) affect NGINX web server components
- Remote attackers can exploit flaws without privileges to execute code or launch denial-of-service attacks on non-default configurations
- Patches available for NGINX Plus, NGINX Open Source, NGINX Ingress Controller, NGINX Gateway Fabric and NGINX Instance Manager
- Temporary mitigations available for organizations unable to patch immediately
- F5 products have been targeted by threat actors in recent years, with eight vulnerabilities exploited

Vulnerability Details

F5 has issued emergency security patches addressing multiple critical vulnerabilities in its NGINX web server platform. Three flaws carry critical severity ratings: two in the `ngx_http_v3_module` component (CVE-2026-15176 and CVE-2026-97205) and one in the NGINX `map` directive (CVE-2026-93479). Remote attackers without authentication can exploit these vulnerabilities on systems running non-default configurations.

Successful exploitation triggers heap-based buffer overflows or use-after-free conditions in the NGINX worker process, resulting in system crashes or forced restarts. More concerning, attackers may achieve arbitrary code execution on systems where Address Space Layout Randomization is disabled or when ASLR protections can be bypassed.

Affected Products and Mitigations

The vulnerabilities affect multiple NGINX software products including NGINX Plus, NGINX Open Source, NGINX Ingress Controller, NGINX Gateway Fabric, and NGINX Instance Manager. F5 has released patches for all affected versions.

For organizations unable to apply patches immediately, F5 has published temporary mitigation measures. CVE-2026-15176 can be mitigated by avoiding the `alias` directive in location blocks and the `$request_filename` variable. CVE-2026-97205 risks can be reduced by disabling asynchronous file I/O or Server Side Includes. CVE-2026-93479 can be addressed by using named captures instead of unnamed captures and limiting their scope.

Threat Context

While F5 has not confirmed active exploitation of these specific vulnerabilities, the company's products have been frequent targets. Since November 2021, eight F5 vulnerabilities have been flagged as actively exploited, with four used in ransomware campaigns. Threat actors have previously exploited F5 flaws to breach networks, map infrastructure, hijack devices, and steal sensitive data. In August 2025, state-sponsored actors breached F5 systems and stole source code and information about undisclosed BIG-IP vulnerabilities.

What to do now

1. Identify all NGINX deployments across your infrastructure, including NGINX Plus, Open Source, Ingress Controller, Gateway Fabric and Instance Manager
2. Apply F5 security patches immediately to all affected NGINX systems, prioritizing internet-facing and critical infrastructure servers

3. For systems that cannot be patched immediately, implement the temporary mitigations published by F5 for each CVE
4. Review NGINX configurations to identify non-default settings that may increase exposure to these vulnerabilities
5. Monitor NGINX systems for unusual crashes, restarts or suspicious worker process behavior that may indicate exploitation attempts
6. Document patching status and mitigation measures for compliance reporting to NCA or SAMA as applicable