Hive Pro

Threat Level

Red

Hiveforce Labs

THREAT ADVISORY

VULNERABILITY REPORT

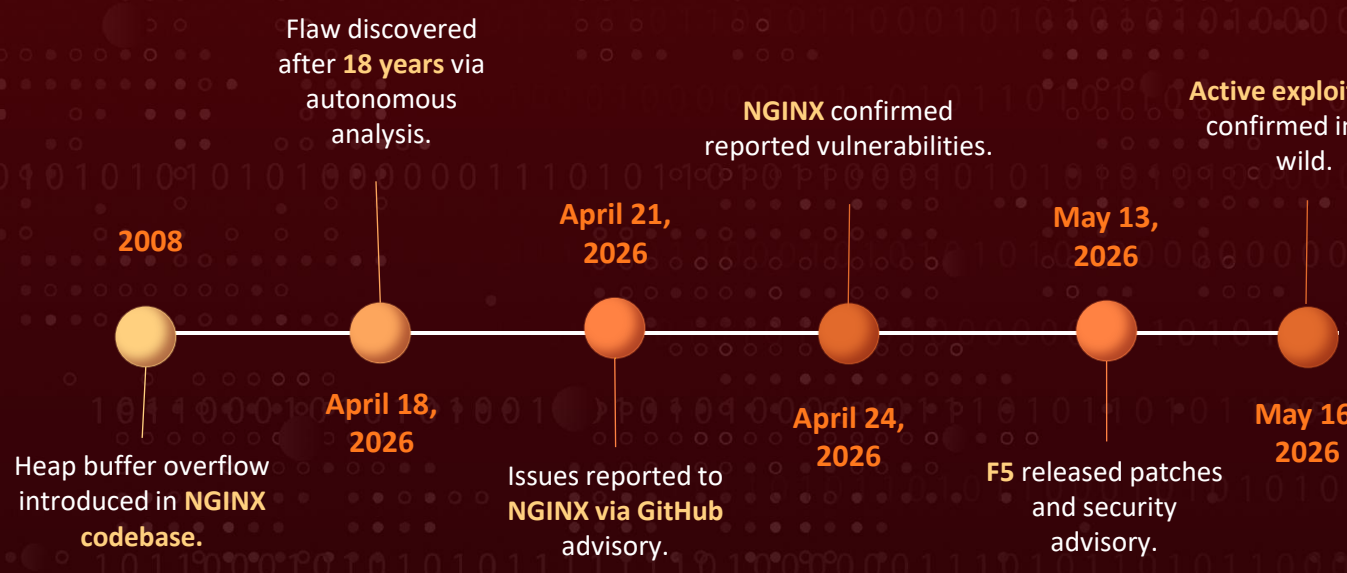
Critical NGINX Vulnerabilities Including 18-Year-Old RCE Flaw Actively Exploited

Date of Publication	Admiralty Code	TA Number
May 18, 2026	A1	TA2026135

Summary

Disclosure Date: May 13, 2026
Affected Products: NGINX Open Source, NGINX Plus, NGINX Instance Manager, F5 WAF for NGINX, NGINX App Protect WAF/DoS, NGINX Gateway Fabric, NGINX Ingress Controller
Impact: F5 has released emergency patches addressing six security vulnerabilities in NGINX, with the most severe being CVE-2026-42945, a critical heap-based buffer overflow in the ngx_http_rewrite_module that remained undetected in the codebase for approximately 18 years since 2008. An unauthenticated attacker can exploit this flaw by sending a single crafted HTTP request to crash NGINX worker processes or, on systems where ASLR is disabled, achieve remote code execution. NGINX powers approximately one-third of all websites globally, and any internet-exposed instance using the vulnerable rewrite pattern is at risk, and since this pattern is common in production deployments, the attack surface remains vast. Active exploitation was confirmed against honeypot networks by May 16, 2026, just four days after disclosure, with a public proof-of-concept already circulating. Organizations running affected versions are strongly urged to upgrade to NGINX patched versions without delay.

Vulnerability Timeline



CVEs

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2026-42945	NGINX Rift (F5 NGINX ngx_http_rewrite_module Heap-Based Buffer Overflow Vulnerability)	F5 NGINX	✗	✗	✓
CVE-2026-42946	F5 NGINX ngx_http_scgi/uwsgi_module Excessive Memory Allocation Vulnerability	F5 NGINX	✗	✗	✓
CVE-2026-40701	F5 NGINX ngx_http_ssl_module OCSP Use-After-Free Vulnerability	F5 NGINX	✗	✗	✓
CVE-2026-42934	F5 NGINX ngx_http_charset_module Out-of-Bounds Read Vulnerability	F5 NGINX	✗	✗	✓
CVE-2026-40460	F5 NGINX HTTP/3 Address Spoofing Vulnerability	F5 NGINX	✗	✗	✓
CVE-2026-42926	F5 NGINX ngx_http_proxy_v2_module HTTP/2 Request Injection Vulnerability	F5 NGINX	✗	✗	✓

Vulnerability Details

#1

A critical set of vulnerabilities affecting NGINX, the world's most widely deployed web server, was publicly disclosed by F5 on May 13, 2026. The most severe among them, CVE-2026-42945, is a heap-based buffer overflow in the ngx_http_rewrite_module that has existed undetected in the NGINX codebase for approximately 18 years since its introduction in 2008. The vulnerability impacts NGINX Open Source versions 0.6.27 through 1.30.0, NGINX Plus R32 through R36, and a broad range of associated F5 products including NGINX Instance Manager, App Protect WAF, Gateway Fabric, and Ingress Controller. NGINX powers approximately one-third of all websites globally, and any internet-exposed instance using the vulnerable rewrite pattern is at risk, and since this pattern is common in production deployments, the attack surface remains vast.

#2

The vulnerability stems from a state mismatch in NGINX's script engine during URL rewriting. When a rewrite directive with a question-mark-containing replacement is followed by a set directive referencing a regex capture, the engine calculates the destination buffer size using one escaping method but writes using another. Escapable characters like plus signs and ampersands expand from one byte to three bytes during the copy pass, overflowing the allocated heap buffer. An unauthenticated attacker can trigger this with a single crafted HTTP request targeting servers that use specific rewrite configuration patterns.

#3

On all affected configurations, successful exploitation crashes the NGINX worker process, causing denial of service. On systems where Address Space Layout Randomization is disabled, the overflow can be leveraged for remote code execution. The attacker exploits NGINX's multi-process architecture, where forked workers share identical memory layouts, to reliably corrupt pool cleanup function pointers and execute arbitrary commands via sprayed fake structures in POST request bodies. A public proof-of-concept demonstrating full RCE has been made available.

#4

By May 16, 2026, active exploitation was confirmed against security honeypot networks, just four days after disclosure. The nature and attribution of the attacks remain unknown. Alongside CVE-2026-42945, five additional NGINX vulnerabilities were patched in the same release: CVE-2026-42946 (excessive memory allocation), CVE-2026-40701 (use-after-free in OCSP handling), CVE-2026-42934 (out-of-bounds read), CVE-2026-40460 (HTTP/3 address spoofing), and CVE-2026-42926 (HTTP/2 request injection) .

#5

F5 released patched versions 1.31.0 and 1.30.1 on May 13, 2026. Organizations are urged to upgrade immediately, audit rewrite configurations, enforce ASLR, and monitor for anomalous HTTP requests targeting rewrite patterns.

Vulnerability

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-42945	NGINX Plus: R32 – R36NGINX Open Source: 1.0.0 – 1.30.0, 0.6.27 – 0.9.7 NGINX Instance Manager: 2.16.0 – 2.22.0F5 WAF for NGINX: 5.9.0 – 5.12.1 NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0F5 DoS for NGINX: 4.8.0 NGINX App Protect DoS: 4.3.0 – 4.7.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2 NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2	cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*:*	CWE-122
CVE-2026-42946	NGINX Plus: R32 – R36 NGINX Open Source: 1.0.0 – 1.30.0, 0.8.42 – 0.9.7 NGINX Instance Manager: 2.16.0 – 2.22.0 F5 WAF for NGINX: 5.9.0 – 5.12.1 NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0 F5 DoS for NGINX: 4.8.0 NGINX App Protect DoS: 4.3.0 – 4.7.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2 NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2	cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*:*	CWE-789
CVE-2026-40701	NGINX Plus: R32 – R36 NGINX Open Source: 1.19.0 – 1.30.0 NGINX Instance Manager: 2.16.0 – 2.22.0 F5 WAF for NGINX: 5.9.0 – 5.12.1 NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0 F5 DoS for NGINX: 4.8.0 NGINX App Protect DoS: 4.3.0 – 4.7.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2 NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2	cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*:*	CWE-416

CVE ID	AFFECTED PRODUCTS	AFFECTED CPE	CWE ID
CVE-2026-42934	NGINX Plus: R32 – R36 NGINX Open Source: 1.0.0 – 1.30.0, 0.3.50 – 0.9.7 NGINX Instance Manager: 2.16.0 – 2.22.0 F5 WAF for NGINX: 5.9.0 – 5.12.1 NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0 F5 DoS for NGINX: 4.8.0 NGINX App Protect DoS: 4.3.0 – 4.7.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2 NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2	cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*	CWE-125
CVE-2026-40460	NGINX Plus: R32 – R36 NGINX Open Source: 1.25.0 – 1.30.0 NGINX Instance Manager: 2.16.0 – 2.22.0 F5 WAF for NGINX: 5.9.0 – 5.12.1 NGINX App Protect WAF: 5.1.0 – 5.8.0, 4.9.0 – 4.16.0 F5 DoS for NGINX: 4.8.0 NGINX App Protect DoS: 4.3.0 – 4.7.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2 NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2	cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*	CWE-290
CVE-2026-42926	NGINX Open Source: 1.29.4 – 1.30.0 NGINX Instance Manager: 2.16.0 – 2.22.0 NGINX Gateway Fabric: 2.0.0 – 2.6.0, 1.3.0 – 1.6.2 NGINX Ingress Controller: 5.0.0 – 5.4.2, 4.0.0 – 4.0.1, 3.5.0 – 3.7.2	cpe:2.3:a:f5:nginx:*:*:*:*:*:*:*:*	CWE-172

Recommendations

Upgrade NGINX Immediately: Apply the patched versions of NGINX without delay. For NGINX Open Source, upgrade to version 1.31.0 (mainline) or 1.30.1 (stable branch). For NGINX Plus users, apply the corresponding patched release as described in the F5 security advisory K000160932. After upgrading, verify the installed version by running the nginx -v command to confirm the fix is in place. Given that active exploitation has been observed in the wild, this upgrade should be treated as an emergency priority.

Apply Configuration Workaround if Immediate Patching Is Not Possible: If upgrading cannot be performed immediately, F5 recommends a configuration-level mitigation. Replace all unnamed PCRE captures ($1, $2, etc.) with named captures in affected rewrite directives. This eliminates the triggering condition for the buffer size miscalculation that leads to the heap overflow. This workaround should be treated as a temporary measure only, and a full upgrade should be completed as soon as operationally feasible.

Audit NGINX Configurations for Vulnerable Patterns: Conduct a thorough review of all NGINX configuration files across the environment to identify instances of the vulnerable pattern — specifically, a rewrite directive using unnamed regex captures with a question-mark-containing replacement string, followed by another rewrite, if, or set directive. Prioritize patching or reconfiguring any instances that match this pattern, particularly those exposed to the public internet.

Verify and Enforce ASLR: Ensure that Address Space Layout Randomization (ASLR) is enabled at the operating system level on all servers running NGINX. ASLR is the primary mitigation that prevents the heap buffer overflow from being escalated to remote code execution. On Linux systems, confirm that /proc/sys/kernel/randomize_va_space is set to 2. While ASLR does not prevent the denial-of-service impact, it significantly raises the difficulty of achieving code execution.

Harden the NGINX Runtime Environment: Ensure NGINX worker processes are running under an unprivileged system account. Enable and enforce mandatory access controls such as AppArmor or SELinux profiles on NGINX processes to limit the damage even if exploitation succeeds. Disable any unused NGINX modules to minimize the attack surface. Review and restrict file permissions on configuration files containing sensitive data such as database credentials.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
Execution	T1203: Exploitation for Client Execution	
Impact	T1499: Endpoint Denial of Service	T1499.004: Application or System Exploitation
Resource Development	T1588: Obtain Capabilities	T1588.006: Vulnerabilities
		T1588.005: Exploits
		T1588.002: Tool
Reconnaissance	T1595: Active Scanning	T1595.002: Vulnerability Scanning
Privilege Escalation	T1068: Exploitation for Privilege Escalation	

Patch Link

https://my.f5.com/manage/s/article/K000161019

https://my.f5.com/manage/s/article/K000161027

https://my.f5.com/manage/s/article/K000161021

https://my.f5.com/manage/s/article/K000161028

https://my.f5.com/manage/s/article/K000161068

https://my.f5.com/manage/s/article/K000161131

https://my.f5.com/manage/s/article/K000160932

References

https://my.f5.com/manage/s/article/K000161019

https://my.f5.com/manage/s/article/K000160932

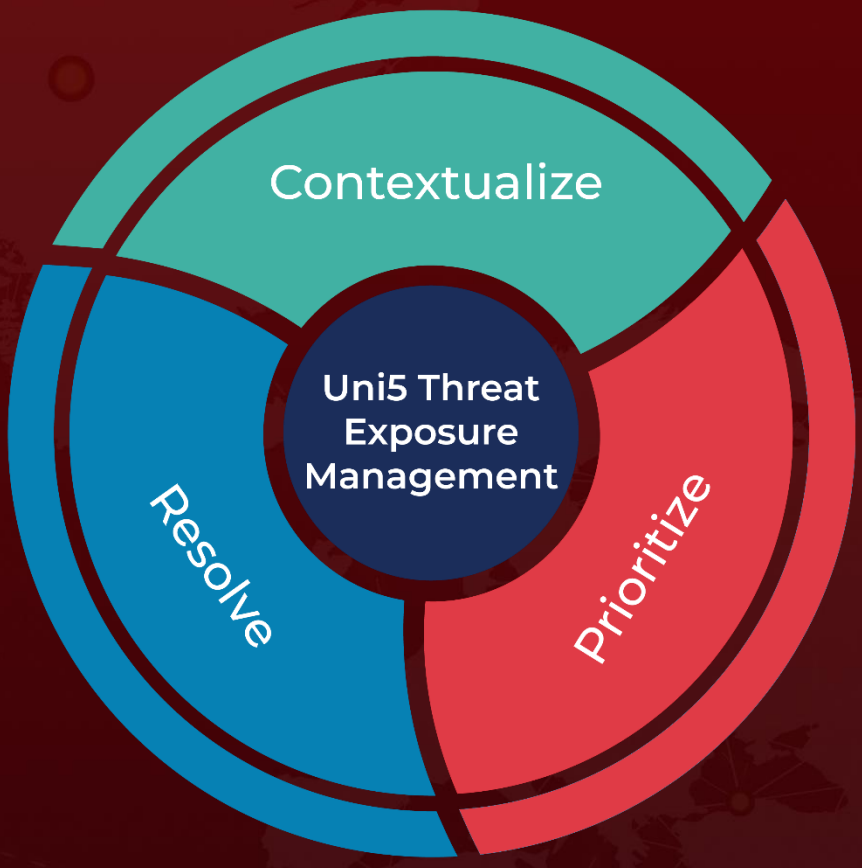
https://depthfirst.com/research/nginx-rift-achieving-nginx-rce-via-an-18-year-old-vulnerability

https://github.com/DepthFirstDisclosures/Nginx-Rift

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

May 18, 2026 • 09:00 PM

More at www.hivepro.com