An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2605150220

NCSC Advisory

F5: NGINX Open Source, NGINX Plus
CVE-2026-42945

15 May 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-42945

Published: 2026-05-13

Vendor: F5

Product: NGINX Open Source, NGINX Plus

CVSS Score[1]: 8.1

Products Affected

Product	Version
NGINX Plus	R36 < R36 P4
NGINX Plus	R32 < R32 P6
NGINX Open Source	0.6.27 < 1.30.1

Impact

NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_rewrite_module module. This vulnerability exists when the rewrite directive is followed by a rewrite, if, or set directive and an unnamed Perl-Compatible Regular Expression (PCRE) capture (for example, $1, $2) with a replacement string that includes a question mark (?). An unauthenticated attacker along with conditions beyond its control can exploit this vulnerability by sending crafted HTTP requests. This may cause a heap buffer overflow in the NGINX worker process leading to a restart. Additionally, for systems with Address Space Layout Randomization (ASLR) disabled, code execution is possible. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.

Common Weakness Enumeration (CWE)[2]: CWE-122: Heap-based Buffer Overflow.

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

---

[1] https://www.first.org/cvss/

[2] https://cwe.mitre.org

[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from F5.

- https://nvd.nist.gov/vuln/detail/CVE-2026-42945
- https://www.cve.org/CVERecord?id=CVE-2026-42945
- https://my.f5.com/manage/s/article/K000161019
- https://depthfirst.com/nginx-rift
- https://github.com/DepthFirstDisclosures/Nginx-Rift