An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2606180233

NCSC Advisory

Mulitiple Serious Vulnerabilities in F5: NGINX Open Source

CVE-2026-42530, CVE-2026-42055

18th, June 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-2026-42530

Published: 2026-06-17

Vendor: F5

Product: NGINX Open Source

CVSS Score[1]: 8.1

Products Affected

Product	Version
NGINX Open Source	1.31.0 < 1.31.2

Impact

NGINX Open Source has a vulnerability in the ngx_http_v3_module module. When NGINX Open Source is configured to use the HTTP/3 QUIC module, a remote unauthenticated attacker along with conditions beyond their control can use a specially crafted HTTP/3 session to reopen a QPACK encoder stream. This may cause a Use-after-Free in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR.

Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.,

Common Weakness Enumeration (CWE)[2]: CWE-416: CWE-416 Use After Free

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

Description

CVE ID: CVE-2026-42055

Published: 2026-06-17

Vendor: F5

Product: NGINX Open Source, NGINX Plus

CVSS Score[4]: 8.1

Products Affected

Product	Version
NGINX Open Source	1.13.10 < 1.31.2
NGINX Open Source	1.30.2 < 1.30.3
NGINX Plus	37.0 < 37.0.2.1
NGINX Plus	R36 < R36 P6

Impact

NGINX Plus and NGINX Open Source have a vulnerability in the ngx_http_proxy_v2_module and ngx_http_grpc_module modules. This vulnerability exists when the proxy_http_version to 2 or grpc_pass directives are used to proxy HTTP/2 traffic, the ignore_invalid_headers directive is set to off, and the large_client_header_buffers directive size is larger than 2 megabytes. A remote, unauthenticated attacker, along with conditions beyond their control, could send large headers while creating an upstream request. This may cause a heap-based buffer overflow in the NGINX worker process leading to a restart. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR.

Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.,

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

Common Weakness Enumeration (CWE)[5]: CWE-122: CWE-122 Heap-based Buffer Overflow

Known Exploited Vulnerability (KEV) catalog[6]: No

Used by Ransomware Operators: N/A

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-2026-42530
- https://www.cve.org/CVERecord?id=CVE-2026-42530
- https://my.f5.com/manage/s/article/K000161616

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

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