An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611180365

NCSC Advisory

F5: NGINX vulnerabilities

18th, November 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-2026-123007

Published: 2026-11-18

Vendor: F5

Product: NGINX Open Source, NGINX Plus

CVSS Score[1]: 8.1

Products Affected

Product	Branch	Version
NGINX Plus	37.x	37.1.0 < 37.3.0.1
NGINX Plus	37.x	37.0.0 < 37.0.8.1
NGINX Plus	Rx	R34-R36
NGINX Open Source	1.x	1.31.0 < 1.31.9
NGINX Open Source	1.x	1.9.5 < 1.30.7

Impact

This issue affects NGINX Plus or NGINX Open Source configurations that use HTTP/2. When NGINX processes undisclosed traffic, the flow control window can exceed the allowed threshold, potentially resulting in a heap buffer overflow typically followed by an NGINX worker segmentation fault. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR.

An attacker could leverage this vulnerability to crash the NGINX worker process, corrupt its memory, or potentially execute code remotely. There is no control plane exposure; this is a data plane issue only.

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

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

Common Weakness Enumeration (CWE)[2]: CWE-191 Integer Underflow (Wrap or Wraparound), CWE-787: Out-of-bounds Write

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

Used by Ransomware Operators: N/A

Description

CVE ID: CVE-2026-123633

Published: 2026-11-18

Vendor: F5

Product: NGINX Open Source, NGINX Plus

CVSS Score: 8.1

Products Affected

Product	Branch	Version
NGINX Plus	37.x	37.1.0 < 37.2.0.1
NGINX Plus	37.x	37.0.0 < 37.0.7.1
NGINX Plus	Rx	R34-R36
NGINX Open Source	1.x	1.31.0 < 1.31.9
NGINX Open Source	1.x	1.19.7 < 1.30.7

Impact

When NGINX Plus or NGINX Open Source is configured to use HTTP/2 for client connections and proxy client requests to a backend, a specially crafted request can result in use-after-free in the worker process, if this process is running low on worker_connections. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR.

[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system or may allow a code execution. There is no control plane exposure; this is a data plane issue only.

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

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

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

Description

CVE ID: CVE-2026-121810

Published: 2026-11-18

Vendor: F5

Product: NGINX Open Source, NGINX Plus

CVSS Score: 8.1

Products Affected

Product	Branch	Version
NGINX Plus	37.x	37.1.0 < 37.3.0.1
NGINX Plus	37.x	37.0.0 < 37.0.8.1
NGINX Plus	Rx	R34 – R36
NGINX Open Source	1.x	1.31.0 < 1.31.9
NGINX Open Source	1.x	1.25.0 < 1.30.7

Impact

This issue affects NGINX Plus and NGINX Open Source configurations that use HTTP/3. A remote, unauthenticated attacker can cause a use-after-free condition in the NGINX worker process, leading to a restart. Exploitation also depends on conditions beyond the attacker's control. Additionally, attackers can execute code on systems with Address Space Layout Randomization (ASLR) disabled or when the attacker can bypass ASLR.

This vulnerability may allow remote attackers to cause a denial-of-service (DoS) on the NGINX system or to possibly trigger a code execution. There is no control plane exposure; this is a data plane issue only.

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

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

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

Description

CVE ID: CVE-2026-123634

Published: 2026-11-18

Vendor: F5

Product: NGINX Open Source, NGINX Plus

CVSS Score: 8.1

Products Affected

Product	Branch	Version
NGINX Plus	37.x	37.1.0 < 37.3.0.1
NGINX Plus	37.x	37.0.0 < 37.0.8.1
NGINX Plus	Rx	R34- R36
NGINX Open Source	1.x	1.31.0 < 1.31.9
NGINX Open Source	1.x	1.0.0 < 1.30.7
NGINX Open Source	0.x	0.6.18 <0.8.55

Impact

This issue occurs when NGINX Plus or NGINX Open Source is configured as a proxy, the proxied server name includes variables, and a Server Side Includes (SSI) or mirror directive sends a subrequest to a location that resolves the same server name. Under these conditions, a specially crafted HTTP request may cause a use-after-free condition in a worker process. An attacker may also be able to execute code if Address Space Layout Randomization (ASLR) is disabled or the attacker can bypass ASLR.

An attacker could leverage this vulnerability to crash the NGINX worker process, corrupt its memory, or perform remote code execution (RCE)

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

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

Known Exploited Vulnerability (KEV) catalog: No

Used by Ransomware Operators: N/A

The following other vulnerabilities have been published by F5:

CVE	Affected Products
BIG-IP iControl REST vulnerability CVE-2026-120718	BIG-IP (all modules)
NGINX TLSv1.3 vulnerability CVE-2026-118899	NGINX Plus, NGINX Open Source
NGINX ngx_mail_proxy_module vulnerability CVE-2026-113425	NGINX Plus, NGINX Open Source
NGINX ngx_stream_ssl_module vulnerability CVE-2026-120993	NGINX Plus, NGINX Open Source
NGINX map directive and regex matching vulnerability CVE-2026-125283	NGINX Plus, NGINX Open Source
NGINX ngx_stream_ssl_module vulnerability CVE-2026-120967	NGINX Plus, NGINX Open Source
NGINX ngx_stream_ssl_preread_module vulnerability CVE-2026-123640	NGINX Plus, NGINX Open Source
BIG-IP and BIG-IQ iControl SOAP vulnerability CVE-2026-125274	BIG-IP (all modules), BIG-IQ Centralized Management
BIG-IP APM vulnerability CVE-2026-123637	BIG-IP APM
BIG-IP APM vulnerability CVE-2026-125272	BIG-IP APM
BIG-IP iRule vulnerability CVE-2026-120285	BIG-IP (all modules), BIG-IP Next for Kubernetes
BIG-IP iRule vulnerability CVE-2026-120292	BIG-IP (all modules), BIG-IP Next for Kubernetes
BIG-IP iRule vulnerability CVE-2026-116953	BIG-IP (all modules), BIG-IP Next for Kubernetes
BIG-IP APM SAML vulnerability CVE-	BIG-IP APM

2026-126822	
BIG-IP APM vulnerability CVE-2026-126336	BIG-IP APM
BIG-IP APM and BIG-IP SSL Orchestrator vulnerability CVE-2026-121812	BIG-IP APM, BIG-IP SSL Orchestrator
BIG-IP iRule vulnerability CVE-2026-120722	BIG-IP DNS, BIG-IP Next for Kubernetes
BIG-IP iRule vulnerability CVE-2026-121805	BIG-IP PEM, BIG-IP Next for Kubernetes

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://my.f5.com/manage/s/article/K000164058
- https://nvd.nist.gov/vuln/detail/CVE-2026-123007
- https://www.cve.org/CVERecord?id=CVE-2026-123007
- https://my.f5.com/manage/s/article/K000163926
- https://nvd.nist.gov/vuln/detail/CVE-2026-123634
- https://www.cve.org/CVERecord?id=CVE-2026-123634
- https://my.f5.com/manage/s/article/K000163925
- https://nvd.nist.gov/vuln/detail/CVE-2026-121810
- https://www.cve.org/CVERecord?id=CVE-2026-121810
- https://my.f5.com/manage/s/article/K000163927
- https://nvd.nist.gov/vuln/detail/CVE-2026-123633
- https://www.cve.org/CVERecord?id=CVE-2026-123633
- https://my.f5.com/manage/s/article/K000163928