INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 14:52 UTC

# F5 NGINX Critical RCE and DoS Vulnerabilities, Emergency Out-of-Band Patches Released

CVE VULNERABILITY | CRITICAL | CVSS 9.5

| | |
|---|---|
| SCC Item ID | SCC-CVE-2026-0326 |
| Type | CVE Vulnerability |
| CVE ID | CVE-2026-42530, CVE-2026-42055, CVE-2026-11311, CVE-2026-50107 |
| Severity | CRITICAL |
| CVSS Base Score | 9.5 |
| EPSS Score | 0.0076 (50th percentile) |
| Affected Products | F5 NGINX Plus, NGINX Open Source, NGINX Gateway Fabric, NGINX Instance Manager |
| Published | 2026-06-18T07:33:00 |
| Discovery Source | Rss |

## Executive Summary

F5 released emergency out-of-band patches on June 18, 2026 for two critical vulnerabilities in NGINX Plus, NGINX Open Source, NGINX Gateway Fabric, and NGINX Instance Manager that allow unauthenticated remote attackers to crash systems or execute arbitrary code. The vulnerabilities affect non-default configurations, but NGINX underpins cloud infrastructure, API gateways, and load balancers across most enterprise environments, making the potential blast radius large. Active exploitation has not been confirmed, but F5 products have prior documented targeting by ransomware operators and nation-state actors, and the out-of-band release signals F5 assessed these as too severe to defer.

## Technical Analysis

F5 issued out-of-band patches for four CVEs: CVE-2026-42530 and CVE-2026-42055 are rated critical (CVSS base 9.5) and enable unauthenticated remote attackers to trigger denial-of-service or remote code execution against affected NGINX deployments under non-default configurations. The CWE profile includes CWE-416 (Use After Free), CWE-122 (Heap-Based Buffer Overflow), and CWE-94 (Improper Control of Code Generation), indicating memory corruption primitives consistent with exploitable RCE chains. CVE-2026-11311 and CVE-2026-50107 are referenced in the same advisory scope; independent severity classification for those two CVEs is not confirmed in available source material. Affected products: F5 NGINX Plus, NGINX Open Source, NGINX Gateway Fabric, and NGINX Instance Manager. MITRE ATT&CK techniques associated with this vulnerability class include T1190 (Exploit Public-Facing Application), T1203 (Exploitation for Client

Execution), T1059 (Command and Scripting Interpreter), T1499/T1499.004 (Endpoint/Application Denial of Service), and T1574 (Hijack Execution Flow). EPSS score is 0.00755 (50th percentile) at time of reporting; CISA KEV listing has not been confirmed. Patches are available as of June 18, 2026 via the F5 security advisory. No public exploit code or confirmed active exploitation has been reported at time of writing.

## Action Checklist

1. Step 1: Containment, Immediately identify all NGINX Plus, NGINX Open Source, NGINX Gateway Fabric, and NGINX Instance Manager instances in your environment using your asset inventory (CIS 1.1, Establish and Maintain Detailed Enterprise Asset Inventory). Restrict external access to any NGINX instances running non-default configurations, particularly those directly internet-exposed without an upstream WAF or IPS, until patching is confirmed complete.
2. Step 2: Detection, Query asset management and CMDB for all NGINX deployments and cross-reference against the affected product list. Review NGINX access logs and error logs for anomalous request patterns, unexpected process crashes, or memory fault indicators. Enable enhanced logging per NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation) on all NGINX hosts. Apply D3-LAM (Local Account Monitoring) and D3-SFA (System File Analysis) to NGINX host processes to detect unauthorized modifications or unexpected child process spawning. Check for signs of T1190 (exploit attempts against public-facing application) in web application firewall and IDS/IPS telemetry.
3. Step 3: Eradication, Apply F5's June 18, 2026 out-of-band patches to all affected instances: NGINX Plus, NGINX Open Source, NGINX Gateway Fabric, and NGINX Instance Manager. Follow the F5 security advisory upgrade path for each product line. Where immediate patching is not possible, review and enforce default-safe configurations as a temporary mitigation, and place affected instances behind a WAF or IPS capable of filtering malformed requests. Reference CIS 7.3 (Perform Automated Operating System Patch Management) and CIS 7.4 (Perform Automated Application Patch Management) for patch deployment process.
4. Step 4: Recovery, After patching, validate that updated NGINX versions are confirmed deployed across all identified instances. Restart services in a controlled sequence and verify application functionality. Monitor NGINX process behavior and system memory metrics for at least 72 hours post-patch for anomalous crashes or restarts that could indicate attempted exploitation against unpatched residual instances. Confirm no unauthorized changes to NGINX configuration files or binaries using D3-SFA (System File Analysis) and D3-FMBV (File Magic Byte Verification). Re-enable full production traffic only after validation is complete.
5. Step 5: Post-Incident, Evaluate whether your asset inventory (CIS 1.1) and software inventory (CIS 2.1, Establish and Maintain a Software Inventory) provided sufficient coverage to identify all NGINX instances quickly. Assess whether patch management processes (CIS 7.3, CIS 7.4) met target remediation timelines for a critical out-of-band advisory. Review whether internet-facing NGINX instances have WAF or IPS coverage as a compensating control. Document any non-default NGINX configurations that increased exposure and evaluate whether those configurations are operationally necessary. Update your vulnerability management process (CIS 7.1) to include out-of-band F5 advisory tracking.

## Detection Guidance

Primary detection focus is on NGINX process anomalies consistent with memory corruption exploitation (CWE-416, CWE-122) and unauthorized code execution (CWE-94). Check NGINX error logs for unexpected segmentation faults, heap corruption messages, or worker process crashes. In SIEM, create alerts for NGINX worker process respawn rates exceeding baseline and for abnormal HTTP request sizes or malformed headers targeting NGINX endpoints. Review host-based IDS telemetry for T1190 indicators: unusual outbound connections initiated by the NGINX process, unexpected child processes spawned by NGINX workers, or new files written by the NGINX process user. For T1574 (Hijack Execution Flow), apply D3-SICA (System Init Config Analysis) to verify NGINX startup configuration integrity and D3-SFA (System File Analysis) to check NGINX binary and module hashes against known-good baselines. Enable AU-6 (Audit Record Review, Analysis, and Reporting) processes to include daily review of NGINX host audit logs. No public IOCs (IPs, domains, hashes) are confirmed at time of reporting; update detection rules as F5 or CISA publish indicators. Monitor CISA's KEV catalog for addition of any of these CVEs, which would indicate confirmed active exploitation.

## Framework Mappings

### MITRE-ATTACK

- **T1499.004** — Application or System Exploitation
- **T1203** — Exploitation for Client Execution
- **T1574** — Hijack Execution Flow
- **T1059** — Command and Scripting Interpreter
- **T1499** — Endpoint Denial of Service
- **T1190** — Exploit Public-Facing Application

### NIST-800-53R5

- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **SC-5** — Denial-of-Service Protection
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-10** — Information Input Validation
- **SI-16** — Memory Protection
- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **IR-5** — Incident Monitoring

### OWASP-TOP10-2021

- **A03:2021** — Injection

### CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

### NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

### HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

### ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.23** — Information security for use of cloud services

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1499.004 | Application or System Exploitation | Impact |
| T1203 | Exploitation for Client Execution | Execution |
| T1574 | Hijack Execution Flow | Persistence |
| T1059 | Command and Scripting Interpreter | Execution |
| T1499 | Endpoint Denial of Service | Impact |
| T1190 | Exploit Public-Facing Application | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/f5-issues-out-of-ban... | T3 |
| **May 2026 CVE Landscape - Recorded Future** | https://www.recordedfuture.com/blog/may-2026-cve-landscape | T3 |
| **NVD** | https://nvd.nist.gov/vuln/detail/CVE-2026-42530, CVE-2026-42055, CV... | T1 |

Generated 2026-06-18 14:52 UTC by TJS Security Command Center