INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 14:31 UTC

CVE-2026-40987: A malicious or compromised FTP/SFTP/SMB server can write arbitrary files anywhere on the client file...

CVE VULNERABILITY | HIGH | CVSS 7.1

SCC Item ID	SCC-CVE-2026-0301
Type	CVE Vulnerability
CVE ID	CVE-2026-40987
Severity	HIGH
CVSS Base Score	7.1
EPSS Score	0.0003 (10th percentile)
Affected Products	Spring Integration 7.0.0-7.0.4; 6.5.0-6.5.8; 6.4.0-6.4.11; 6.3.0-6.3.14; 5.5.0-5.5.20
Published	2026-06-11T07:16:27.053
Discovery Source	Nvd

Executive Summary

CVE-2026-40987 is a path traversal vulnerability in Spring Integration's remote file synchronization components, affecting versions across the 5.5, 6.3, 6.4, 6.5, and 7.0 release lines. Any application using Spring Integration to synchronize files from a remote FTP, SFTP, or SMB server is at risk: if that server is malicious or becomes compromised, an attacker can write arbitrary files anywhere on the client host, including web shells, backdoors, or overwritten configuration files. The business risk is unauthorized system access, potential full host compromise, and persistent attacker presence on internal infrastructure.

Technical Analysis

CVE-2026-40987 is a server-to-client path traversal vulnerability (CWE-22) in Spring Integration's remote file synchronization components for FTP, SFTP, and SMB protocols. Affected versions: Spring Integration 7.0.0-7.0.4, 6.5.0-6.5.8, 6.4.0-6.4.11, 6.3.0-6.3.14, and 5.5.0-5.5.20. The vulnerability arises because the synchronization components do not sufficiently validate or sanitize filenames returned by the remote server before writing files to the local filesystem. A malicious or attacker-controlled remote server can return filenames containing directory traversal sequences (e.g., '../../') that resolve outside the configured local-directory, writing attacker-controlled content to arbitrary filesystem locations. Exploitation requires that the Spring Integration client connect to a compromised or adversary-controlled FTP/SFTP/SMB server; it is not directly

internet-exploitable unless the application is configured to sync from an untrusted external server. Potential outcomes include web shell placement (T1190), configuration file overwrite (T1565.001), and staging of additional payloads (T1105). CVSS base score: 7.1 (High). EPSS: 0.034% (10.5th percentile). Not currently listed on CISA KEV. No public exploit code confirmed in source data.

Action Checklist

1. Containment: Immediately audit all Spring Integration deployments running affected versions (7.0.0-7.0.4, 6.5.0-6.5.8, 6.4.0-6.4.11, 6.3.0-6.3.14, 5.5.0-5.5.20). Suspend or isolate any application instances that synchronize files from external or untrusted FTP/SFTP/SMB servers until patching is confirmed. If suspension is not possible, restrict outbound connections from affected hosts to only trusted, internally controlled file servers (NIST AC-4, Information Flow Enforcement; CIS 4.4, Implement and Manage a Firewall on Servers).
2. Detection: Audit the local directories configured as sync targets for unexpected files, particularly in parent directories or sensitive paths (e.g., /etc, web roots, application config directories). Query file integrity monitoring logs for new or modified files outside expected sync boundaries. Review application logs for Spring Integration file adapter activity and look for filenames containing traversal sequences ('..', '%2e%2e', URL-encoded variants). Enable or verify file system auditing on affected hosts (NIST AU-2, Event Logging; NIST SI-4 equivalent monitoring; CIS 8.2, Collect Audit Logs; D3-SFA, System File Analysis).
3. Eradication: Upgrade Spring Integration to the patched release for your version line. Consult the official Spring Integration release page (spring.io/projects/spring-integration) and the Spring Security Advisory for your affected branch to confirm the minimum patched version. After upgrading, validate that the synchronization components enforce local-directory boundaries by testing with a controlled filename containing traversal sequences (NIST SI-2, Flaw Remediation; CIS 7.3, Perform Automated Operating System Patch Management; CIS 7.4, Perform Automated Application Patch Management).
4. Recovery: After patching, scan all previously configured sync-target directories and their parent paths for unexpected files written during the exposure window, prioritizing web roots, cron directories, SSH authorized_keys files, and application configuration paths. Remove any files not consistent with expected sync content. Rotate credentials and SSH keys on affected hosts if any indication of unauthorized file placement is found. Re-enable file server connections only after confirming the remote server's integrity (NIST AU-6, Audit Record Review, Analysis, and Reporting; D3-CRO, Credential Rotation).
5. Post-Incident: Review the trust model for all remote file server connections in Spring Integration deployments: treat any external file server as potentially hostile and implement server identity verification. Assess whether file integrity monitoring (FIM) coverage extends to sync-target directories and their parent paths. Review least-privilege configurations for the application service account to limit the blast radius of arbitrary file writes (NIST AC-6, Least Privilege; CIS 5.4, Restrict Administrator Privileges to Dedicated Administrator Accounts; D3-UAP, User Account Permissions; D3-SFA, System File Analysis).

Detection Guidance

Query file integrity monitoring (FIM) or EDR telemetry for new or modified files created by the Spring Integration application process outside the configured sync local-directory. Specifically look for file creation events in sensitive paths: web roots, /etc, application configuration directories, cron/at directories, and SSH directories.

Search application and framework logs for filenames containing path traversal patterns: literal '..', URL-encoded '%2e%2e%2f', or backslash variants '..\'. On Linux hosts, use auditd rules targeting the application service account UID to log all file write syscalls (open with O_WRONLY/O_RDWR, rename, link) outside the expected sync directory tree. On Windows, enable Object Access auditing on parent directories above the sync target. Behavioral indicator: files appearing in locations the sync process has no legitimate reason to write, timed to coincide with remote file synchronization job execution. No public IOCs (IPs, domains, hashes) are available in the source data for this CVE; detection relies on filesystem and process behavior, not network signatures (D3-SFA, System File Analysis; NIST AU-2, Event Logging; CIS 8.2, Collect Audit Logs).

Framework Mappings

MITRE-ATTACK

- **T1565.001** — Stored Data Manipulation
- **T1105** — Ingress Tool Transfer
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **SI-10** — Information Input Validation

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **16.12** — Implement Code-Level Security Checks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1565.001	Stored Data Manipulation	Impact

Technique ID	Technique Name	Tactic
T1105	Ingress Tool Transfer	Command-And-Control
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
nvd	https://nvd.nist.gov/vuln/detail/CVE-2026-40987	T1
CVE-2026-40987: Spring Integration Remote-File Synchronizer File ...	https://www.herodevs.com/blog-posts/cve-2026-40987-spring-integrati...	T3
CVE-2026-40987 - CVE Record	https://www.cve.org/CVERecord?id=CVE-2026-40987	T3
CVE-2026-40987 - High Vulnerability - TheHackerWire	https://www.thehackerwire.com/vulnerability/CVE-2026-40987/	T3

Generated 2026-06-15 14:31 UTC by TJS Security Command Center