BLACKSWAN CYBERSECURITY

THREAT ADVISORY
Splunk Enterprise Remote Code Execution
September 2, 2026

Severity: Critical (CVSS 9.8)
CVE: CVE-2026-20253
Affected Product: Splunk Enterprise 10.x
Status: Patch Immediately

Executive Summary

Splunk released emergency security updates for a critical vulnerability, **CVE-2026-20253**, affecting certain versions of Splunk Enterprise. The flaw exists within a PostgreSQL sidecar service used by Splunk Enterprise and allows a **remote, unauthenticated attacker** to create or truncate arbitrary files on the target system. Researchers have demonstrated that the vulnerability can be chained into **pre-authentication remote code execution (RCE)**, allowing complete compromise of affected Splunk servers.

The vulnerability stems from a lack of authentication controls on a PostgreSQL sidecar service endpoint, enabling any network-reachable attacker to invoke file operations without valid credentials. Splunk's Product Security Incident Response Team (PSIRT) has reported awareness of **limited exploitation activity** as of June 2026.

Because Splunk servers often serve as centralized logging, SIEM, and security monitoring platforms, successful exploitation could allow attackers to:

- Disable or manipulate security monitoring
- Delete or corrupt evidence of malicious activity
- Access sensitive log and telemetry data
- Establish persistence
- Pivot deeper into enterprise networks
- Execute arbitrary operating system commands on the host system

Affected Versions

Vulnerable

Product	Versions
Splunk Enterprise 10.0	10.0.0 - 10.0.6
Splunk Enterprise 10.2	10.2.0 - 10.2.3

THREAT ADVISORY
Splunk Enterprise Remote Code Execution
September 2, 2026

Not Vulnerable

Product	Status
Splunk Enterprise 10.4	**Not affected**
Splunk Enterprise 9.4 and earlier	**Not affected**
Splunk Cloud Platform	**Not affected**

Fixed Versions

- Splunk Enterprise 10.0.7+
- Splunk Enterprise 10.2.4+
- Splunk Enterprise 10.4.0+

Technical Analysis

Root Cause

The vulnerability is classified as:

- **CWE-306: Missing Authentication for Critical Function**
- **CVSS v3.1: 9.8 (Critical)**

The PostgreSQL sidecar service exposes administrative endpoints that permit file operations without requiring authentication. Any attacker capable of reaching these endpoints can create or truncate files on the underlying operating system. [advisory.splunk.com], [hellorecon.com]

Attack Chain

Researchers from watchTowr Labs demonstrated a path to pre-authentication RCE:

1. Connect Splunk to an attacker-controlled PostgreSQL database.
2. Abuse the /backup endpoint to place malicious database content on the Splunk server.
3. Use the /restore endpoint with a crafted passfile parameter.
4. Leverage Splunk's .pgpass credentials to gain interaction with the local PostgreSQL instance.
5. Execute attacker-controlled SQL during restoration.
6. Use PostgreSQL's lo_export() functionality to write arbitrary files.
7. Overwrite scripts, configuration files, or executable content, ultimately enabling remote code execution.

THREAT ADVISORY
Splunk Enterprise Remote Code Execution
September 2, 2026

MITRE ATT&CK Mapping / TTPs

Initial Access

T1190 - Exploit Public-Facing Application

Attackers exploit exposed Splunk endpoints without authentication.

Execution

T1059 - Command and Scripting Interpreter

Attackers can achieve operating system command execution by writing or modifying executable scripts.

Persistence

T1505.003 - Web Shell

Adversaries may place web-accessible scripts or webshells in reachable directories.

T1053.003 - Scheduled Task/Cron

Potential creation of cron jobs or scheduled execution mechanisms.

Defense Evasion

T1070 - Indicator Removal on Host

Attackers may truncate or destroy logs and evidence stored on the Splunk server.

Impact

T1485 - Data Destruction

Arbitrary file truncation can erase indexes, logs, configurations, and evidence.

T1499 - Endpoint Denial of Service

Critical Splunk services may become unavailable through file destruction.

THREAT ADVISORY
Splunk Enterprise Remote Code Execution
September 2, 2026

Indicators of Compromise (IOCs)

Network Indicators

Monitor for requests to:

1 /v1/postgres/recovery/backup
2 /v1/postgres/recovery/restore

These endpoints were specifically identified during proof-of-concept exploitation.

File Indicators

Unexpected creation or modification of:

1 /opt/splunk/var/packages/data/postgres/.pgpass

Unexpected modifications to:

1 server.conf
2 inputs.conf
3 transforms.conf
4 splunk-launch.conf

Unexpected files appearing in:

1 $SPLUNK_HOME/etc/
2 $SPLUNK_HOME/bin/
3 web-accessible directories

Behavioral Indicators

Process Activity

Investigate:

- Child processes spawned from splunkd
- Shell execution by Splunk service accounts
- Unexpected Python execution
- Database restore operations outside maintenance windows

Configuration Changes

Detect:

- Unauthorized modifications to Splunk configuration files
- New scheduled searches
- Unexpected changes to PostgreSQL sidecar components

Detection Recommendations

Splunk Log Review

Review:

spl isn't fully supported. Syntax highlighting is based on Plain Text.
1 index=_internal
2 index=_audit

Look for:

- Unusual PostgreSQL recovery activity
- Unauthorized restore jobs
- Unexpected administrative actions
- Configuration changes

Endpoint Detection

Monitor for:

- File writes performed by Splunk processes
- New executable content written by postgres-related services
- Modifications to Splunk binaries or scripts
- Abnormal outbound connections from Splunk servers

Remediation

Immediate Actions

1. Patch Immediately

Upgrade to:

- Splunk Enterprise 10.0.7+
- Splunk Enterprise 10.2.4+
- Splunk Enterprise 10.4.0+

2. Restrict Network Access

Limit access to Splunk management and web interfaces to trusted administrative systems.

Examples include:

8000/TCP
8089/TCP
9997/TCP

3. Disable PostgreSQL Sidecar (Temporary Mitigation)

If immediate patching is not possible:

INI
[postgres]
disabled = true

Add to:

$SPLUNK_HOME/etc/system/local/server.conf

Restart Splunk after the change.

Warning: Do not use this workaround if the instance relies on:

- Edge Processor
- OpAmp
- SPL2 Data Pipelines

4. Hunt for Post-Exploitation Activity

Review:

- Unauthorized file creation

- Webshell deployment
- Suspicious cron tasks
- Privilege escalation activity
- Log tampering events

Risk Assessment

Category	Rating
Exploitability	Critical
Authentication Required	None
User Interaction	None
Network Exposure	Remote
Privileges Required	None
Business Impact	Severe
Detection Difficulty	Moderate

A compromised Splunk deployment can provide adversaries visibility into security telemetry, detection rules, credentials, and monitoring infrastructure. Organizations operating internet-accessible Splunk management interfaces should treat this vulnerability as a **Priority-1 emergency patching event**.

Organizations that identify vulnerable Splunk deployments or suspect compromise should act quickly to validate exposure, contain potential threats, and verify the integrity of their security monitoring infrastructure. **Blackswan Cybersecurity** can assist throughout the entire incident lifecycle, including emergency vulnerability assessments, Splunk hardening and remediation, threat hunting, compromise assessments, log and forensic analysis, malicious persistence detection, and incident response activities. Our team can help determine whether exploitation has occurred, identify indicators of compromise, restore trust in affected Splunk environments, and implement continuous monitoring and detection capabilities to reduce future risk. For organizations requiring additional support, Blackswan also provides managed detection and response (MDR), security operations center (SOC) services, vulnerability management, and executive-level incident advisory services to help ensure rapid containment and recovery from critical threats such as CVE-2026-20253.