

Alert Bulletin

Bulletin N.: 105

Publication Date: 21/09/2026

Subject: Alert 2026-105 Pre-authenticated RCE Vulnerability in Splunk Enterprise

Traffic Light Protocol (TLP): White

Affected product(s):

Product	Affected versions	Fixed version
Splunk Enterprise	10.0.0 to 10.0.6	10.0.7 or later
Splunk Enterprise	10.2.0 to 10.2.3	10.2.4 or later
Splunk Enterprise	10.4	Not affected
Splunk Cloud Platform	Not affected	Not applicable

*The vulnerability only affects Splunk Enterprise using the PostgreSQL *sidecar* component. **Splunk Cloud Platform is not affected**, since it does not use *Postgres sidecars*.

Description

A vulnerability labeled **CVE-2026-20253** was identified, a critical vulnerability in **Splunk Enterprise** with a **CVSS 9.8** score. The flaw allows a remote unauthenticated attacker to perform arbitrary file operations through an exposed endpoint of the PostgreSQL *sidecar* service and, through an attack chain, achieve **remote code execution (RCE)** on the Splunk server.

CVE-2026-20253 occurs because the PostgreSQL *sidecar* service endpoint lacks authentication controls. Any actor able to reach the service over the network can invoke file operations without providing credentials. [thehackernews](https://thehackernews.com/2026/09/splunk-enterprise-rce-vulnerability.html)

The vulnerability allows creating or truncating arbitrary files and can be chained to achieve pre-authentication RCE. The endpoints involved in the disclosed technical chain are:

```
/v1/postgres/recovery/backup  
/v1/postgres/recovery/restore
```

The research team demonstrated that an attacker can use the `/backup` endpoint to connect to a PostgreSQL database under their control and save a *dump* to an arbitrary path on the Splunk server's file system. Subsequently, they can invoke `/restore`, leveraging a local `.pgpass` file containing the

postgres_admin account password, to restore attacker-controlled content into the local PostgreSQL instance.

Although initially there were no reports of exploitation, the Splunk Product Security Incident Response Team (**PSIRT**) reported on June 18, 2026 that it had knowledge of **limited exploitation** of the vulnerability. CISA added CVE-2026-0253 to its Known Exploited Vulnerabilities (**KEV**) catalog, so immediate updating is recommended, along with reviewing potential indicators of compromise.

Solution

- **Update Splunk Enterprise immediately** to a fixed version:
- 10.0.0–10.0.6 → update to **10.0.7 or higher**.
- 10.2.0–10.2.3 → update to **10.2.4 or higher**.
- Splunk Enterprise 10.4 → not affected.

<https://advisory.splunk.com/advisories/SVD-2026-0603>

<https://docs.splunk.com/Documentation/Splunk/X/Installation/HowtoupgradeSplunk>

<https://docs.splunk.com/Documentation/Splunk/X/Admin/Serverconf>

<https://docs.splunk.com/Documentation/Splunk/X/Admin/Postgresqlconf>

- **Identify all affected Splunk Enterprise instances**, including *search heads*, *indexers*, management nodes, standalone servers, contingency environments, laboratories, and third-party deployments. Confirm whether each instance uses the PostgreSQL *sidecar*.
- **Restrict exposure of PostgreSQL sidecar endpoints and ports**. Limit access to strictly authorized administrative networks and Splunk components; block any access from the Internet, user networks, guest segments, and non-administrative VPNs. This measure reduces exposure while patching is completed, but does not replace updating.
- **Review network, proxy, and Splunk logs** to detect suspicious HTTP requests to:

/v1/postgres/recovery/backup

/v1/postgres/recovery/restore

- Investigate requests originating from unauthorized IPs, unplanned backup/restore patterns, or anomalous responses.
- **Audit the integrity of critical Splunk files**. Verify recent modifications, especially in application directories, Python scripts, configuration files, scheduled tasks, binaries, temporary directories, and paths associated with PostgreSQL recovery.
- **Search for persistence and post-compromise activity**. Review unknown processes, anomalous outbound connections, new or modified credentials/tokens, changes in administrative roles, *forwarder* configurations, alerts, *saved searches*, *lookups*, and installed applications.
- **Rotate secrets and credentials** if indicators of compromise exist. Include Splunk administrative credentials, API tokens, deployment keys, integration secrets, certificates, database credentials, and service accounts used by *forwarders* or connectors.

Additional information:

- <https://thehackernews.com/2026/06/critical-splunk-enterprise-flaw-lets.html>
- <https://advisory.splunk.com/advisories/SVD-2026-0603>