

Multiple Vulnerabilities in Splunk Products



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	183
Authors	Adrian Emanuel Rotaru < adrian.emanuel@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-22
Issue Date	2026-10-22

Threat Reports are reports created by Smarttech247 based on high and critical severity vulnerabilities that may have a high potential to be exploited in the wild i.e. vulnerabilities that are present in most used products by companies and do not have an auto-update option or they are usually not automatically updated in case that could lead to some service disruption. This report is usually created as soon as the vulnerability is released, therefore we strongly recommend that the information is reviewed, tests are performed and patches are applied before the first proof-of-concept is released. Even though certain vulnerabilities may not have an active exploit in the wild at the time that we report on them, we take into consideration the wider risk and the impact it could have on systems, should an exploit like that be available after a while. Our duty is to report them on time and we recommend enterprises that, in order to keep critical business systems protected, they should consider, on average, ten working days to check whether or not the new vulnerability affects them, and if so, to implement actions in order to remove the risk.

Overview:

Multiple security vulnerabilities have been disclosed in Splunk products as part of Splunk's October 2026 security release. The vulnerabilities affect Splunk Enterprise and Splunk Secure Gateway, with fixes delivered in Splunk Enterprise versions 10.4.4, 10.2.8, 10.0.11, and 9.4.16. The release includes both externally reported vulnerabilities (SVD-2026-1007) and internally identified issues addressed through a security hardening release (SVD-2026-1008).

The disclosed issues include remote code execution, improper access control, missing authorization, authorization bypass, SPL injection, cross-site request forgery (CSRF), use of a hard-coded cryptographic key, denial-of-service (DoS), improper resource lifecycle control, protection mechanism failures, and improper neutralization flaws. The most severe vulnerabilities, CVE-2026-76299 (Improper Access Control) and CVE-2026-76302 (Improper Neutralization), each carry a CVSS score of 9.9. Among the externally reported flaws, the most severe is CVE-2026-76298 (CVSS 8.8), which could allow a user without the "admin" or "power" roles to derive the PostgreSQL sidecar superuser password and run arbitrary OS commands as the Splunk service account on search head cluster members.

Successful exploitation of these vulnerabilities could allow attackers or low-privileged users, depending on the specific flaw, to execute arbitrary code or operating-system commands, bypass authorization and access controls, read or delete data outside their ownership scope, bypass SPL safeguards, modify configurations in unauthorized apps, trigger unauthorized state changes via CSRF, disrupt service availability, or otherwise compromise affected Splunk deployments.

Risk

Government:

- Large and medium government entities: **Critical**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **Critical**
- Small business entities: **High**

Technical summary

CVE ID	Description
CVE-2026-76287: Authorization Bypass in the Data Management REST API in Splunk Enterprise CVSSv3.1 Score: 5.4, Medium	In Splunk Enterprise versions below 10.4.4, a user that holds a role with the <code>preview_data_management_pipeline</code> capability or <code>edit_data_management_pipeline_job</code> capability could read or delete Data Management SPL2 preview jobs and results outside their ownership scope. The vulnerability is possible because the Data Management Representational State Transfer (REST) API verifies the required capability but does not verify that the requested preview job belongs to the requester. The affected Data Management REST API is available only when the Edge Processor feature is turned on. The Edge Processor feature is turned off by default. For more information see Set up a data management control plane and Getting sample data for previewing data transformations in the Splunk documentation .
CVE-2026-76288: Denial of Service (DoS) through Splunk Web Content-Type Header Parsing in Splunk Enterprise EnterprisePermalink CVSSv3.1 Score: 7.5, High	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, an unauthenticated user could send a single crafted request to the Splunk Web JavaScript logger endpoint and cause Splunk Web to stop responding to requests. Splunk Web remains unavailable until Splunk Enterprise is restarted. The vulnerability is possible because Splunk Web does not limit request-header parsing before processing the request.
CVE-2026-76289: Denial of Service (DoS) through the REST API in Splunk Enterprise CVSSv3.1 Score: 6.5, Medium	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, a user who does not hold the “admin” or “power” Splunk roles could make the Splunk Enterprise instance unavailable to other users by sending a request to the Representational State Transfer (REST) API endpoint for lookup table files. The affected instance requires a restart to restore service. The vulnerability is possible because the endpoint does not limit resource use when it processes response field selections. For more information see Endpoints reference list and About configuring role-based user access in the Splunk documentation .
CVE-2026-76290: Denial of Service (DoS) through Unauthenticated Package Downloads over the REST API in Splunk Enterprise EnterprisePermalink CVSSv3.1 Score: 7.5, High	In Splunk Enterprise versions below 10.4.4, 10.2.8, and 10.0.11, an unauthenticated user could send repeated requests to the Edge Processor package download endpoint in the Splunk Pipeline Builders app. The requests could cause the Splunk daemon to consume excessive system resources and potentially stop responding. The vulnerability is possible because the endpoint accepts package download requests without authentication and reads and base64-encodes the complete package in memory for each request. After upgrading, prepare all existing Edge Processor instances, turn on authentication for Edge Processor package downloads, and restart Splunk Enterprise. For more information, see Enable authentication for Edge Processor package downloads .
CVE-2026-76291: Improper Access Control through Scheduled Search Safeguards in	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, a user that holds a role with the <code>schedule_search</code> capability could bypass the expected safeguards in the scheduled search workflow. The user could then run risky Search Processing Language (SPL) commands that disclose or alter Splunk Enterprise data or

Splunk Enterprise CVSSv3.1 Score: 8.8, High	disrupt Splunk Enterprise availability. The vulnerability is possible because the Splunk Enterprise search scheduler does not apply SPL safeguards for risky commands to scheduled searches. For more information see SPL safeguards for risky commands in the Splunk documentation. For more information see authorize.conf in the Splunk documentation.
CVE-2026-76292: Missing Authorization through REST API Endpoints in Splunk Secure Gateway CVSSv3.1 Score: 6.5, Medium	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, and Splunk Secure Gateway versions below 3.10.12, 3.9.26, and 3.8.73, a low-privileged user that does not hold the “admin” Splunk role or the “sc_admin” Splunk Secure Gateway role could read mobile alert notification data for other users through Splunk Secure Gateway App Key Value Store (KV Store) Representational State Transfer (REST) API endpoints. The vulnerability is possible because the affected Splunk Secure Gateway App Key Value Store collections do not enforce user-level authorization for read requests. For more information see About the app key value store and About configuring role-based user access in the Splunk documentation.
CVE-2026-76293: Remote Code Execution (RCE) through Splunk Web Manager Extensible Markup Language (XML) in Splunk Enterprise CVSSv3.1 Score: 7.2, High	In Splunk Enterprise versions below 10.4.3, 10.2.8, 10.0.11, and 9.4.16, a user that holds a role with the edit_manager_xml capability could execute arbitrary operating-system commands using the permissions of the user account running Splunk Enterprise by opening the affected configuration in the Splunk Web Manager page. The vulnerability is possible because Splunk Web evaluates user-controlled expressions from Manager XML without sufficiently restricting the expression syntax.
CVE-2026-76294: Improper Access Control in Field Extraction Management in Splunk Enterprise CVSSv3.1 Score: 4.3, Medium	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, a user who does not hold the “admin” or “power” Splunk roles could move field extractions or field transformations to apps for which the user does not have read access. The vulnerability is possible because the Representational State Transfer (REST) API does not validate destination app access before it processes field extraction and field transformation move operations. For more information see Use the Field extractions page and Manage knowledge object permissions in the Splunk documentation.
CVE-2026-76295: SPL Injection through the REST API in Splunk Secure GatewayPermalink CVSSv3.1 Score: 4.3, Medium	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, and Splunk Secure Gateway versions below 3.10.12, 3.9.26, and 3.8.73, a user who does not hold the “admin” or “power” Splunk roles could view dashboard and report listings beyond the requested filter scope while remaining within objects that the user can access. The vulnerability is possible because Splunk Secure Gateway does not neutralize special characters in values before it creates filters for dashboard and report requests. For more information see About configuring role-based user access in the Splunk documentation.
CVE-2026-76296: Missing Authorization through Sourcetype Renaming in Splunk Web for Splunk Enterprise	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, a user who does not hold the “admin” or “power” Splunk roles could create, move, edit, or delete sourcetype renaming configurations that they own in apps that they do not have permission to access. The vulnerability is possible when Splunk Web is turned on because Splunk Web does not verify the required app permissions

CVSSv3.1 Score: 4.3, Medium	before it performs sourcetype renaming operations. For more information see Rename source types at search time in the Splunk documentation.
CVE-2026-76297: Federated Search Provider State Change through Cross-Site Request Forgery (CSRF) in Splunk Web for Splunk Enterprise CVSSv3.1 Score: 4.2, Medium	In Splunk Enterprise versions below 10.4.4, 10.2.8, 10.0.11, and 9.4.16, an unauthenticated user could trick a user that holds a role with the edit_federated_providers capability into turning off all federated search providers. Successful exploitation could temporarily prevent federated searches from retrieving data from remote datasets. The vulnerability is possible because the federated provider Representational State Transfer (REST) API accepts GET requests for actions that change provider state. The vulnerability requires the attacker to phish the affected user by tricking them into initiating a request within their browser. The unauthenticated user should not be able to exploit the vulnerability at will. For more information see Run federated searches over remote Splunk platform deployments and Define roles on the Splunk platform with capabilities in the Splunk documentation.
CVE-2026-76298: Use of Hard-coded Cryptographic Key in the PostgreSQL Sidecar Service in Splunk Enterprise CVSSv3.1 Score: 8.8, High	In Splunk Enterprise versions below 10.4.4 and 10.2.8, a user who does not hold the “admin” or “power” Splunk roles could derive the PostgreSQL sidecar database superuser password and run arbitrary operating system commands as the user account running Splunk Enterprise on search head cluster members. The vulnerability is possible because the PostgreSQL sidecar service derives a privileged database password from the search head cluster identifier that appears in search job logs. For more information see About configuring role-based user access, server.conf, and Sidecar configuration settings in the Splunk documentation.
Improper Access Control CVE-2026-76299 Highest CVSS Score: 9.9	
Improper Control of a Resource Through its Lifetime CVE-2026-76300 Highest CVSS Score: 8.8	
Protection Mechanism Failure CVE-2026-76301 Highest CVSS Score: 7.6	
Improper Neutralization CVE-2026-76302 Highest CVSS Score: 9.9	

Affected products

Product	Base Version	Affected Version	Fix Version
Splunk Enterprise	10.4	10.4.0 to 10.4.3	10.4.4
	10.2	10.2.0 to 10.2.7	10.2.8

	10.0	10.0.0 to 10.0.10	10.0.11
	9.4	9.4.0 to 9.4.15	9.4.16

Recommendations

We recommend the following actions be taken:

- Apply appropriate updates, hot fixes or mitigations provided by Splunk to vulnerable systems immediately after appropriate testing. ([M1051: Update Software](#))
 - **Safeguard 7.1: Establish and Maintain a Vulnerability Management Process:** Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
 - **Safeguard 7.2: Establish and Maintain a Remediation Process:** Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
 - **Safeguard 7.4: Perform Automated Application Patch Management:** Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
 - **Safeguard 7.5: Perform Automated Vulnerability Scans of Internal Enterprise Assets:** Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.
 - **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
 - **Safeguard 12.1: Ensure Network Infrastructure is Up-to-Date:** Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.
 - **Safeguard 18.1: Establish and Maintain a Penetration Testing Program:** Establish and maintain a penetration testing program appropriate to the size, complexity, and maturity of the enterprise. Penetration testing program characteristics include scope, such as network, web application, Application Programming Interface (API), hosted services, and physical premise controls; frequency; limitations, such as acceptable hours, and excluded attack types; point of contact information; remediation, such as how findings will be routed internally; and retrospective requirements.
 - **Safeguard 18.2: Perform Periodic External Penetration Tests:** Perform periodic external penetration tests based on program requirements, no less than annually. External penetration testing must include enterprise and environmental reconnaissance to detect exploitable information. Penetration testing requires specialized skills and experience and must be conducted through a qualified party. The testing may be clear box or opaque box.
 - **Safeguard 18.3: Remediate Penetration Test Findings:** Remediate penetration test findings based on the enterprise's policy for remediation scope and prioritization.
- Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic. ([M1037: Filter Network Traffic](#))
 - **Safeguard 4.2: Establish and Maintain a Secure Configuration Process for Network Infrastructure:** Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.
 - **Safeguard 7.6: Perform Automated Vulnerability Scans of Externally-Exposed**

- Enterprise Assets:** Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.
- **Safeguard 7.7: Remediate Detected Vulnerabilities:** Remediate detected vulnerabilities in software through processes and tooling on a monthly, or more frequent, basis, based on the remediation process.
- Use capabilities to detect and block conditions that may lead to or be indicative of a software exploit occurring. (**M1050: Exploit Protection**)
 - **Safeguard 10.5: Enable Anti-Exploitation Features:** Enable anti-exploitation features on enterprise assets and software, where possible, such as Microsoft® Data Execution Prevention (DEP), Windows® Defender Exploit Guard (WDEG), or Apple® System Integrity Protection (SIP) and Gatekeeper™.

References

<https://advisory.splunk.com/advisories/SVD-2026-1007>
<https://advisory.splunk.com/advisories/SVD-2026-1008>

CVE

CVE-2026-76291
CVE-2026-76298
CVE-2026-76288
CVE-2026-76290
CVE-2026-76293
CVE-2026-76289
CVE-2026-76292
CVE-2026-76287
CVE-2026-76294
CVE-2026-76295
CVE-2026-76296
CVE-2026-76297
CVE-2026-76299
CVE-2026-76300
CVE-2026-76301
CVE-2026-76302

