

Multiple Vulnerabilities in Splunk Products



Document ID	SMA-Threat Report
Document status	ISSUED
Issue Number	177
Authors	Dorin Constantin Banu < constantin.banu@smarttech247.com >
Verified by	Alin Curcan < alin.curcan@smarttech247.com >
Last modified	2026-10-09
Issue Date	2026-10-07

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 September/October 2026 Security Hardening Release. The vulnerabilities affect Splunk Enterprise, Splunk Secure Gateway, Splunk App Observability Cloud, Discover Splunk Observability Cloud, and Splunk App O11y Cloud.

The disclosed issues include remote code execution, improper access control, privilege escalation, authorization bypass, SQL injection, server-side request forgery (SSRF), log injection, denial-of-service (DoS), information disclosure, and input validation flaws. The most severe vulnerability, CVE-2026-76268, carries a CVSS score of 9.8.

Successful exploitation of these vulnerabilities could allow attackers or low-privileged users, depending on the specific flaw, to execute arbitrary code, gain elevated privileges, bypass authorization controls, access sensitive information, perform SQL injection or SSRF attacks, manipulate logs and configurations, 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-2026-76264 CVSS Score: 4.3 Improper Authorization through the REST API in Splunk Enterprise	In Splunk Enterprise versions below 10.4.2, 10.2.6, 10.0.10, and 9.4.15, a user who does not hold the "admin" or "power" Splunk roles could create or edit scripted lookup definitions through raw configuration endpoints. The vulnerability is possible because raw transforms configuration write paths do not apply external lookup capability checks before saving scripted lookup settings.

CVE-2026-76265 CVSS Score: 6.5 Improper Access Control through REST API Endpoints in Splunk Secure Gateway	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, and Splunk Secure Gateway versions below 3.10.11, 3.9.25, and 3.8.72, a user who does not hold the “admin” or “power” Splunk roles could access privileged Splunk Secure Gateway functionality. With this access, the user could cause Splunk Secure Gateway to sign attacker-controlled payloads. The vulnerability is possible because multiple Splunk Secure Gateway Representational State Transfer (REST) API endpoints do not enforce authorization requirements before processing requests.
CVE-2026-76266 CVSS Score: 7.7 Local Privilege Escalation through Linux Package Upgrades in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15 on Linux, a local user who can run commands as the user account running Splunk Enterprise could cause an affected Linux package upgrade to run attacker-controlled operating-system commands with root privileges. The vulnerability is possible because the Linux package maintainer script trusts existing Splunk Enterprise installation content when it performs upgrade operations with root privileges. The vulnerability requires an affected Linux package upgrade to occur after the local user modifies the installation. The local user should not be able to elevate privileges at will.
CVE-2026-76267 CVSS Score: 4.3 Log Injection through the REST API in Splunk App for Splunk O11y Cloud	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a user that holds a role with the read_o11y_content capability could inject forged entries into the app log through the Representational State Transfer (REST) API. The vulnerability is possible because Splunk App for Splunk O11y Cloud does not neutralize user-supplied SignalFlow content before writing it to the app log.
CVE-2026-76268 CVSS Score: 9.8 Missing Authentication for Critical Function in the Patroni REST API in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3 and 10.2.7, an unauthenticated user with network access to the Patroni Representational State Transfer (REST) Application Programming Interface (API) on a search head cluster member could execute attacker-controlled operating-system commands. The vulnerability is possible because this interface does not require authentication for critical configuration operations. For more information see Sidecar configuration settings in the Splunk documentation.
CVE-2026-76269 CVSS Score: 6.5 Improper Access Control in Search Job Retrieval through the REST API in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user who does not hold the “admin” or “power” Splunk roles could use a user-controlled job identifier to access substantially all search job information from jobs that belong to other users, including search query text, job metadata, results, and preview results, through an Application Programming Interface (API) implemented as a Representational State Transfer (REST) API. The vulnerability is possible because the REST API does not fully validate job ownership before returning search job information.
CVE-2026-76270 CVSS Score: 6.5 Structured Query Language (SQL) Injection in the SPL2 Module Catalog in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, a user that holds a role with the list_spl2_modules capability could use SQL injection in SPL2 module filtering to access all relevant data available through the affected Representational State Transfer (REST) API, including private SPL2 module definitions belonging to other users. The vulnerability is possible because Splunk Enterprise and Splunk Cloud Platform do not parameterize user-supplied values before using them in database

	queries for SPL2 module filtering. For more information see Manage SPL2 modules and Module permissions in the Splunk documentation.
CVE-2026-76271 CVSS Score: 6.5 Denial of Service (DoS) in the Discover Splunk Observability Cloud app for Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a low-privileged user that does not hold the “admin” or “power” Splunk roles could cause a denial of service against a Representational State Transfer (REST) API endpoint in the Discover Splunk Observability Cloud app. The vulnerability is possible because the app uses an inefficient regular expression to validate input submitted through the endpoint. For more information see About configuring role-based user access , Splunk Observability Cloud previews , and restmap.conf in the Splunk documentation.
CVE-2026-76272 CVSS Score: 4.3 Missing Access Control through the REST API in Splunk Secure Gateway	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user who does not hold the “admin” or “power” Splunk roles could cause Splunk Secure Gateway to sign attacker-controlled payloads. The vulnerability is possible because Splunk Secure Gateway does not verify that the user is authorized to request a signature. Splunk Secure Gateway versions below 3.10.11, 3.9.25, and 3.8.72 are also affected. For more information see Define roles on the Splunk platform with capabilities in the Splunk documentation.
CVE-2026-76273 CVSS Score: 4.3 Improper Input Validation through the collect Command in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user that holds a role with the run_collect capability could use the collect Search Processing Language (SPL) command to add attacker-controlled content to system-level messages on the Splunk platform instance. The vulnerability is possible because the collect command does not validate the index name before processing the value. For more information see collect , Define roles on the Splunk platform with capabilities , and System endpoint descriptions in the Splunk documentation.
CVE-2026-76274 CVSS Score: 6.5 Server-Side Request Forgery (SSRF) through the REST API in Splunk App for Splunk Observability Cloud	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a user that holds a role with the read_o11y_content capability could redirect an outbound request from Splunk App for Splunk Observability Cloud through the Representational State Transfer (REST) API to an attacker-controlled host and disclose the configured Observability Cloud Application Programming Interface (API) token. The vulnerability is possible because Splunk App for Splunk Observability Cloud does not fully validate the destination of an outbound request. For more information see Authentication tokens in the Splunk documentation.
CVE-2026-76275 CVSS Score: 4.3 Improper Authorization in Search Job Listings through the REST API in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user who does not hold the “admin” or “power” Splunk roles could access search query text and job metadata for jobs that belong to other users, including job identifiers, dispatch parameters, result counts, and execution metadata, through an Application Programming Interface (API) implemented as a Representational State Transfer (REST) API. The vulnerability is possible because the REST API does not fully enforce per-user authorization before it includes job information in search job listings.
CVE-2026-76276	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a low-privileged user that does not hold the “admin” or “power” Splunk

CVSS Score: 4.3 Information Disclosure in the Discover Splunk Observability Cloud app through Splunk Web for Splunk Enterprise	roles could retrieve original source code for the Discover Splunk Observability Cloud app through Splunk Web. The vulnerability is possible because production JavaScript bundles for the app contain embedded source maps that include original source code. For more information see About configuring role-based user access, Splunk Observability Cloud previews, and Navigating Splunk Web in the Splunk documentation.
CVE-2026-76277 CVSS Score: 4.1 Improper Input Validation of Native Splunk Usernames through the REST API in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user that holds a role with the edit_user capability could create a native Splunk username that ends with a period. The vulnerability is possible because username validation does not reject a trailing period before the username is used for a user directory. This can cause distinct native Splunk usernames to share per-user configuration data, and user-management operations can affect the wrong account or fail. For more information see Set up native Splunk authentication and Define roles on the Splunk platform with capabilities in the Splunk documentation.
CVE-2026-76278 CVSS Score: 4.3 Authorization Bypass in SPL2 Module Permissions in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, and 10.0.10, a user that holds a role with the edit_spl2_module_permissions capability could use the affected Representational State Transfer (REST) API to access permission grants for SPL2 modules that the user does not have permission to view. The vulnerability is possible because Splunk Enterprise does not verify that the user can read the requested app before the affected REST API returns SPL2 module permission grants. For more information see Module permissions and Manage SPL2 modules in the Splunk documentation.
CVE-2026-76279 CVSS Score: 4.3 Improper Input Validation of Index Names through the collect Command in Splunk Enterprise	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, a user that holds a role with the run_collect capability could use the collect Search Processing Language (SPL) command to write events to internal indexes outside the index access configured for the role. The vulnerability is possible because Splunk Enterprise does not normalize whitespace in an index name before applying configured index-access restrictions for the role. For more information see collect, Define roles on the Splunk platform with capabilities, and How indexing works in the Splunk documentation.
CVE-2026-76280 CVSS Score: 6.3 Incorrect Permission Assignment for App Key Value Store Collections in Splunk Secure Gateway	In Splunk Enterprise versions below 10.4.3, 10.2.7, 10.0.10, and 9.4.15, and Splunk Secure Gateway versions below 3.10.11, 3.9.25, and 3.8.72, an authenticated user who does not hold the “admin” or “sc_admin” Splunk roles could modify Splunk Secure Gateway alert and mobile-device recipient data in App Key Value Store (KV Store) collections that later alert and subscription workflows use. The vulnerability is possible because the affected collections allow unrestricted write access instead of limiting writes to authorized Splunk Secure Gateway workflows. For more information see About the app key value store, KV store endpoint descriptions, and About configuring role-based user access in the Splunk documentation.

Affected products

Product	Base Version	Affected Version	Fix Version
Splunk Enterprise	10.4	10.4.0 to 10.4.2	10.4.3
	10.2	10.2.0 to 10.2.6	10.2.7
	10.0	10.0.0 to 10.0.9	10.0.10
	9.4	9.4.0 to 9.4.14	9.4.15

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-2026-1001?utm_source=chatgpt.com#cve-2026-76264

CVE

CVE-2026-76264
 CVE-2026-76265
 CVE-2026-76266
 CVE-2026-76267
 CVE-2026-76268
 CVE-2026-76269
 CVE-2026-76270
 CVE-2026-76271
 CVE-2026-76272
 CVE-2026-76273
 CVE-2026-76274
 CVE-2026-76275
 CVE-2026-76276
 CVE-2026-76277
 CVE-2026-76278
 CVE-2026-76279
 CVE-2026-76280

