INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-15 14:30 UTC

# Critical Splunk Enterprise Flaw Lets Attackers Run Code Without Authentication

SECURITY ANALYSIS | CRITICAL | CVSS 9.8

| | |
|---|---|
| SCC Item ID | SCC-STY-2026-0211 |
| Type | Security Analysis |
| Severity | CRITICAL |
| CVSS Base Score | 9.8 |
| Affected Products | Splunk Enterprise (specific versions not confirmed from available sources, check advisory.splunk.com for affected version ranges) |
| Published | 20 hours ago |
| Discovery Source | Serper |

## Executive Summary

Splunk has issued security updates for a critical vulnerability in Splunk Enterprise carrying a CVSS base score of 9.8. The flaw allows an unauthenticated attacker with network access to execute arbitrary code directly on affected Splunk instances, requiring no credentials or prior foothold. Organizations running Splunk Enterprise should treat this as a priority patch event; a compromised Splunk deployment exposes security monitoring data, stored credentials, and the broader network infrastructure Splunk indexes.

## Technical Analysis

The vulnerability is classified under CWE-306 (Missing Authentication for Critical Function) and maps to MITRE ATT&CK techniques T1190 (Exploit Public-Facing Application) and T1059 (Command and Scripting Interpreter). CVSS base score is 9.8, indicating network-accessible exploitation with no authentication, no user interaction, and high impact across confidentiality, integrity, and availability. No CVE ID was present in the source data and none has been independently verified upstream; the authoritative identifier and affected version ranges must be confirmed at advisory.splunk.com. The attack vector allows a remote, unauthenticated actor to reach an exposed Splunk Enterprise listener and execute arbitrary code at the privilege level of the Splunk process. Patch details, including specific fixed version numbers, are pending confirmation from the Splunk Security Advisory. Source data originates from T3 reporting (news outlets and social media); treat the Splunk advisory as the ground truth for remediation specifics. CVSS vector will be populated once the CVE is published to NVD.

## Action Checklist

1. Step 1, Containment: Immediately restrict network access to Splunk Enterprise management and web ports (default 8000/tcp, 8089/tcp, 9997/tcp) at the perimeter and host firewall to trusted management IP ranges only. This aligns with NIST AC-4 (Information Flow Enforcement) and CIS 4.4. Do not wait for patch details, firewall rules are your immediate control.
2. Step 2, Detection: Query Splunk's own _audit and _internal logs for anomalous unauthenticated requests, unexpected process spawns from splunkd, or new scheduled searches created by unknown principals. Review web access logs on port 8000 for unusual POST requests or encoded payloads. Monitor splunkd process activity and configuration file changes (inputs.conf, transforms.conf) for unauthorized modifications. See NIST AU-6 (Audit Record Review, Analysis, and Reporting) for audit review procedures.
3. Step 3, Eradication: Retrieve patch details from the Splunk Security Advisory at advisory.splunk.com. Subscribe to Splunk security alerts if not already subscribed. Before deploying the patch in production, test it in a non-production environment to validate compatibility. Follow CIS 7.3 and CIS 7.4 for patch management workflows. Verify patch integrity before deployment. If the advisory provides indicators of compromise (IOCs), cross-reference logs against those IOCs to confirm whether exploitation occurred.
4. Step 4, Recovery: After patching, confirm splunkd is running the updated version via the 'splunk version' CLI command. Rotate all Splunk service account credentials and API tokens (aligns with NIST AC-2 Account Management). Re-enable network access incrementally, validating that no anomalous process activity persists. Enable NIST AU-12 (Audit Record Generation) to ensure post-patch activity is fully logged.
5. Step 5, Post-Incident: Review whether Splunk Enterprise management interfaces were internet-facing in violation of CIS 4.4 and NIST AC-17 (Remote Access) controls. Evaluate whether least-privilege principles (NIST AC-6) were applied to the Splunk service account. Update vulnerability management processes per CIS 7.1 to include SIEM platforms in critical-asset patch SLAs. Assess whether multi-factor authentication (CIS 6.5) is enforced on all Splunk administrative access.

## Detection Guidance

Query Splunk _internal and _audit indexes for unauthenticated session attempts, unexpected search job creation by null or anonymous principals, and process spawns from splunkd that invoke system shells (cmd.exe, powershell.exe, /bin/sh, /bin/bash). Alert on HTTP 200 responses to unauthenticated POST requests against /en-US/splunkd/__raw/ or similar API endpoints. Monitor changes to Splunk app directories and configuration files (inputs.conf, transforms.conf) that were not initiated through change-controlled deployment.
Cross-reference NIST AU-6 review cadence for Splunk infrastructure logs. Once the CVE ID and indicators of compromise are published in the Splunk security advisory, add them to your detection rules. Until then, prioritize unauthenticated RCE attempts and unexpected code execution on Splunk hosts as high-risk indicators; reference the Splunk advisory for specific signatures once available.

## Framework Mappings

### MITRE-ATTACK

- **T1059** — Command and Scripting Interpreter
- **T1190** — Exploit Public-Facing Application

### NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **IA-2** — Identification and Authentication (Organizational Users)

### OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures

### CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management

### HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication

### SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

### ISO-27001-2022

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

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1059 | Command and Scripting Interpreter | Execution |
| T1190 | Exploit Public-Facing Application | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| | https://thehackernews.com/2026/06/critical-splunk-enterprise-flaw-l... | T3 |

| Source | URL | Tier |
|---|---|---|
| **Critical Splunk Enterprise Flaw Lets Attackers Run Code Without ...** | https://x.com/evanderburg/status/2065792607939395784/photo/1 | T3 |
| **Splunk Vulnerability Disclosure - Splunk Security Advisories** | https://advisory.splunk.com/?301=%2Fen_us%2Fproduct-security.html | T3 |
| **Splunk Enterprise for Windows Vulnerability Allows SYSTEM Access** | https://www.linkedin.com/posts/cybersecurity-news_cybersecuritynews... | T3 |
| **Splunk Enterprise had an unauthenticated RCE sitting in ... - Reddit** | https://www.reddit.com/r/cybersecurity/comments/1u4rpju/splunk_ente... | T3 |



Generated 2026-06-15 14:30 UTC by TJS Security Command Center