



ThreatCure

Cyber Threat Advisory

Splunk Vulnerability

---

CVE-2024-53247

## Description

# Splunk Vulnerability

### CATEGORY

Vulnerability

### SEVERITY

High

### Platforms

Splunk Enterprise  
Splunk Cloud Platform

### IMPACT

- **RCE Risk:** Low-privileged users can execute arbitrary code remotely.
- **Enterprise Impact:** Potential data breaches and system compromise.
- **Urgent Patch:** High severity (CVSS 8.8), requiring immediate updates.

A serious vulnerability (CVE-2024-53247) has been found in the Splunk Secure Gateway app, which allows low-privileged users to execute remote code due to unsafe deserialization in the jsonpickle Python library. This flaw affects specific versions of **Splunk Enterprise** (below 9.3.2, 9.2.4, and 9.1.7) and the **Splunk Secure Gateway app** on the **Splunk Cloud Platform** (below 3.2.461 and 3.7.13). With a high CVSSv3.1 score of 8.8, it poses a significant threat to organizations using Splunk for log management and SIEM. Users should upgrade to the latest patched versions immediately. For temporary mitigation, users who don't rely on features like Splunk Mobile, Spacebridge, or Mission Control can disable or remove the Secure Gateway app.

This issue emphasizes the need for timely software updates and security best practices. Since Splunk is widely used in enterprise environments, the vulnerability could have a broad impact across industries. Organizations are urged to apply patches without delay to minimize the risk of exploitation and protect against emerging cybersecurity threats.



## Mitigation

- To mitigate the risk associated with the vulnerability, users should **update to the latest patched versions** of **Splunk Enterprise** (9.3.2, 9.2.4, or 9.1.7) and **Splunk Secure Gateway app** (3.2.461 and 3.7.13 or higher). Splunk has released security patches to address this flaw and prevent potential exploitation. For those who do not require **Splunk Mobile**, **Spacebridge**, or **Mission Control** functionalities, disabling or removing the **Splunk Secure Gateway app** can serve as a temporary mitigation.
- **Reference:** For more details, please visit [Splunk's official advisory and patch notes](#) or refer to the security documentation for the specific patch release. Additionally, consult the Manage app and add-on objects documentation for guidance on managing and disabling the [Secure Gateway app](#).

ThreatCure

# Cyber Threat Advisory

---

Secure your byte world



## Splunk Vulnerability

---

CVE-2024-53247

Get Started Today

For more information about the ThreatCure ShieldOps Platform  
or to schedule a demo, please contact:

- Website: [www.threatcure.net](http://www.threatcure.net)
- Email: [info@threatcure.net](mailto:info@threatcure.net)

