Smarttech
YOUR 24/7 SECURITY PARTNER

Critical Splunk RCE Vulnerability – 12th March 2026

Document ID	SMA-Threat Report-Critical Splunk RCE Vulnerability
Document status	ISSUED
Issue Number	21
Authors	Andrei Constantinescu <andrei.constantinescu@smarttech247.com>
Verified by	Alexandru Sandu < alexandru@smarttech247.com >
Last modified	2026-03-12
Issue Date	2026-03-12

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:

A high-severity remote command execution (RCE) vulnerability has been discovered in Splunk Enterprise and Splunk Cloud Platform, exposing enterprise environments to potential system compromise.

The vulnerability, tracked as CVE-2026-20163 and assigned a CVSS score of 8.0, allows attackers to execute arbitrary shell commands on the host operating system if specific privilege conditions are met.

This category of vulnerability occurs when software fails to properly sanitize user-supplied input before passing it to system commands, potentially enabling attackers to inject malicious instructions.

If exploited successfully, the flaw could allow threat actors to run unauthorized commands on affected Splunk servers, potentially leading to full system takeover.

Currently there are no exploitation reports available nor POCs released.

Risk

Government:

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

Businesses:

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

Technical summary

Product	Base Version	Component	Affected Version	Fix Version
Splunk Enterprise	10.2	REST API	Not affected	10.2.0
Splunk Enterprise	10.0	REST API	10.0.0 to 10.0.3	10.0.4
Splunk Enterprise	9.4	REST API	9.4.0 to 9.4.8	9.4.9
Splunk Enterprise	9.3	REST API	9.3.0 to 9.3.9	9.3.10
Splunk Cloud Platform	10.2.2510	REST API	Below 10.2.2510.5	10.2.2510.5

The vulnerability, identified as CVE-2026-20163, resides within a specific Splunk REST API endpoint: /splunkd/__upload/indexing/preview. This component is responsible for generating data previews when users upload new files to the platform.

During the preview phase, Splunk utilizes a parameter called unarchive_cmd to handle compressed or archived files. Security researchers discovered that this parameter does not strictly sanitize input. Consequently, an attacker could theoretically inject malicious shell commands into a file upload request, which the underlying operating system would then execute during the preview process.

Despite the potential for Remote Code Execution (RCE), the exploit path contains a significant security barrier. **A successful attack requires the perpetrator to already possess an authenticated session with edit_cmd capabilities.**

In a standard Splunk environment, this privilege is reserved for high-level administrators. This requirement effectively shifts the threat profile: while it protects against unauthorized external actors, it underscores the importance of securing administrative credentials against phishing or credential stuffing.

Recommendations

Smarttech247 team recommend the following actions be taken:

Apply the latest patches:

- Upgrade Splunk Enterprise 10.0 to version 10.0.4
- Upgrade Splunk Enterprise 9.4 to version 9.4.9
- Upgrade Splunk Enterprise 9.3 to version 9.3.10

Limiting privileged access and enforcing strong authentication controls can help reduce the likelihood of exploitation if credentials are compromised.

References

https://advisory.splunk.com/advisories/SVD-2026-0302

Smarttech
YOUR 24/7 SECURITY PARTNER

www.smarttech247.com