CERT-EU

Security Advisory 2024-111

Multiple Vulnerabilities in Splunk Enterprise and Splunk Cloud

2024-10-16 — v1.0

TLP:CLEAR

History:

- *16/10/2024 — v1.0 – Initial publication*

Summary

On October 14, 2024, Splunk released several advisories addressing multiple high and medium severity vulnerabilities affecting Splunk Enterprise and Splunk Cloud. These vulnerabilities could lead to arbitrary file write to Windows system root directory, access to potentially restricted data and remote code execution [1,2].

Technical Details

The vulnerability **CVE-2024-45733**, with a CVSS score of 8.8, could allow a low-privileged user that does not hold the "admin" or "power" Splunk roles to perform a Remote Code Execution (RCE) due to an insecure session storage configuration.

The vulnerability **CVE-2024-45731**, with a CVSS score of 8.0, could allow a low-privileged user that does not hold the "admin" or "power" Splunk roles to write a file to the Windows system root directory, which has a default location in the Windows `System32` folder, when Splunk Enterprise for Windows is installed on a separate drive. The user could potentially write a malicious DLL which, if loaded, could result in a remote execution of the code within that DLL.

The vulnerability **CVE-2024-45732**, with a CVSS score of 7.1, could allow a low-privileged user that does not hold the "admin" or "power" Splunk roles to run a search as the "nobody" Splunk user in the SplunkDeploymentServerConfig app. This could let the low-privileged user access potentially restricted data.

Please refer to https://advisory.splunk.com/ for the complete list of vulnerabilities.

Affected Products

- The vulnerability **CVE-2024-45733** affects the Splunk Web component of Splunk Enterprise for Windows versions 9.2.0 to 9.2.2, and 9.1.0 to 9.1.5.
- The vulnerability **CVE-2024-45731** affects the Splunk Web component of Splunk Enterprise for Windows versions 9.3.0, 9.2.0 to 9.2.2, and 9.1.0 to 9.1.5 if the Splunk Enterprise instance is installed on a separate disk.
- The vulnerability **CVE-2024-45732** affects the SplunkDeploymentServerConfig component Splunk for Cloud Platform, and Splunk Enterprise versions 9.2.0 to 9.2.2, and 9.3.0.

Recommendations

It is recommended updating affected assets as soon as possible, prioritising Internet facing devices.

It is also recommended:

- disabling the Splunk Web component on indexers in distributed environments;
- restricting write access to knowledge objects within Splunk apps by modifying the local.meta file in the `$SPLUNK_HOME/etc/apps/SplunkDeploymentServerConfig/metadata` directory as follows:

```
[]
access = read : [ * ], write : [ admin ]
```

References

[1] https://advisory.splunk.com/

[2] https://cybersecuritynews.com/splunk-vulnerabilities-remote-code/