CERT-EU

Security Advisory 2023-034

Multiple Vulnerabilities in Splunk Enterprise

June 6, 2023 — v1.0

TLP:CLEAR

History:

- *06/06/2023 — v1.0 – Initial publication*

Summary

On June 6, 2023, Splunk issued security updates to fix several vulnerabilities, 5 of which are being classified as high. These vulnerabilities could lead to privilege escalation, path traversal, local privilege escalation, denial of service or HTTP response splitting [1].

CERT-EU highly recommends updating Splunk as soon as possible to the latest version.

Technical Details

- **CVE-2023-32707**

The vulnerability identified as `CVE-2023-32707` [2], with a CVSS score of 8.8 out of 10, could allow a low-privileged user who holds a role that has the `edit_user` capability assigned, to escalate his/her privileges to that of the admin user by providing a specially crafted web request. This is because the `edit_user` capability does not honour the `grantableRoles` setting in the `authorize.conf` configuration file, which prevents this scenario from happening.

- **CVE-2023-32714**

The vulnerability identified as `CVE-2023-32714` [3], with a CVSS score of 8.1 out of 10, could allow a low-privileged user with access to the Splunk App for Lookup File Editing to trigger a path traversal exploit, with a specially crafted web request, which can then be used to read and write to restricted areas of the Splunk installation directory.

- **CVE-2023-32713**

The vulnerability identified as `CVE-2023-32713` [4], with a CVSS score of 7.8 out of 10, could allow a low-privileged user to escalate his/her privileges on the machine that runs the Splunk Enterprise instance, up to and including the root user.

- **CVE-2023-32706**

The vulnerability identified as `CVE-2023-32706` [5], with a CVSS score of 7.7 out of 10, could allow an unauthenticated attacker to cause a denial of service in the Splunk daemon by sending specially crafted messages to the XML parser within SAML authentication. This happens when an incorrectly configured XML parser receives XML input that contains a reference to an entity expansion. Many recursive references to entity expansions can cause the XML parser to use all available memory on the machine, causing the Splunk daemon to crash or be terminated by the operating system.

- **CVE-2023-32708**

The vulnerability identified as `CVE-2023-32708` [6], with a CVSS score of 7.2 out of 10, could allow a low-privileged user to trigger an HTTP response splitting vulnerability with the `rest` SPL command that lets him/her potentially access other REST endpoints in the system arbitrarily, including viewing restricted content.

Affected Products

The following products are affected by one or more vulnerabilities listed in the Splunk advisory:

- Splunk Enterprise <9.0.5, <8.2.11 and <8.1.14
- Splunk Cloud Platform <9.0.2303.100
- Splunk App for Lookup File Editing versions <4.0.1
- Splunk App for Stream versions <8.1.1

Recommendations

CERT-EU highly recommends updating affected versions of Splunk Enterprise and Apps as soon as possible.

References

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

[2] https://nvd.nist.gov/vuln/detail/CVE-2023-32707

[3] https://nvd.nist.gov/vuln/detail/CVE-2023-32714

[4] https://nvd.nist.gov/vuln/detail/CVE-2023-32713

[5] https://nvd.nist.gov/vuln/detail/CVE-2023-32706

[6] https://nvd.nist.gov/vuln/detail/CVE-2023-32708