Overall rating: High

This notification is intended as an informational bulletin for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware of multiple vulnerabilities reported on Splunk Enterprise and Splunk Cloud Platform.

Technical Details

- **DoS Vulnerability -** CVE-2023-32706
  On Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14 and Splunk Cloud Platform below 9.0.2303.100, an unauthenticated attacker can send specially crafted messages to the XML parser within SAML authentication to cause a denial of service in the Splunk daemon**.**
- **Privilege Escalation Vulnerability** - CVE-2023-32707
  In versions of Splunk Enterprise below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform below version 9.0.2303.100, a low-privileged user who holds a role that has the 'edit_user' capability assigned to it can escalate their privileges to that of the admin user by providing specially crafted web requests.
- **Remote HTTP Response Splitting Vulnerability** - CVE-2023-32708
  In Splunk Enterprise versions below 9.0.5, 8.2.11, and 8.1.14, and Splunk Cloud Platform versions below 9.0.2303.100, a low-privileged user can trigger an HTTP response splitting vulnerability with the 'rest' SPL command that lets them potentially access other REST endpoints in the system arbitrarily**.**

These vulnerabilities are rated as an overall **High** Severity.

Recommended Action

- Investigate how your area of responsibility is affected.
- Notify business owner(s) as required.
- Ensure mitigation is performed at your next change window.

Please notify VRM with any questions or concerns you may have.

References

- https://advisory.splunk.com/advisories/SVD-2023-0601
- https://advisory.splunk.com/advisories/SVD-2023-0602
- https://advisory.splunk.com/advisories/SVD-2023-0603
- https://research.splunk.com/application/e615a0e1-a1b2-4196-9865-8aa646e1708c/
- https://research.splunk.com/application/39e1c326-67d7-4c0d-8584-8056354f6593/