November 17, 2023

Overall rating: High

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team has been made aware of Juniper Secure Analytics vulnerabilities. The vulnerability affects Juniper Secure Analytics versions prior to 7.5.0 UP7.

Technical Details

Multiple vulnerabilities have been resolved. The impact of this vulnerability may allow an attacker to cause denial of service or privilege escalation, access out of bounds memory, potentially access sensitive information. There are no known workarounds for these issue

Exploitability Metrics
Attack Vector: Network
Attack Complexity: Low
Privileges Required: None
User Interaction: None

This vulnerability is rated as a **HIGH** risk. A software update, Juniper Secure Analytics 7.5.0 UP7 IF02 exists to address this risk.

Action Required

- Locate the device or application and investigate.
- Notify business owner(s).
- Perform mitigating actions, as required.

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

References

- CVE-2020-22218, CVE-2023-20593, CVE-2023-35788, CVE-2022-44729, CVE-2023-20900, CVE-2023-3341, CVE-2023-3899, CVE-2023-43057
- 2023-11 Security Bulletin: JSA Series: Multiple vulnerabilities resolved
- VRM Vulnerability Reports