March 5, 2024

Overall rating: Critical

This is a technical bulletin intended for technical audiences.

Summary

The Vulnerability and Risk Management (VRM) Team is aware that SolarWinds published a security advisory to address vulnerabilities in the following product:

- SolarWinds Security Event Manager – versions prior to 2023.4.1

Technical Details
A path traversal vulnerability was identified in Samba when processing client pipe names connecting to Unix domain sockets within a private directory. Samba typically uses this mechanism to connect SMB clients to remote procedure call (RPC) services like SAMR LSA or SPOOLSS, which Samba initiates on demand. However, due to inadequate sanitization of incoming client pipe names, allowing a client to send a pipe name containing Unix directory traversal characters (../).

This could result in SMB clients connecting as root to Unix domain sockets outside the private directory. If an attacker or client managed to send a pipe name resolving to an external service using an existing Unix domain socket, it could potentially lead to unauthorized access to the service and consequential adverse events, including compromise or service crashes.

.

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

This vulnerability is rated as a **CRITICAL** risk. A software update exists to address these risks.

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-2024-0692 CVE-2023-48795 CVE-2023-3961 CVE-2023-4154 CVE-2023-42670
- SolarWinds Security Advisory – sem_2023-4-1_release_notes
- SolarWinds Security Advisories