Overall Rating - High

BRITISH COLUMBIA

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

Summary

The Vulnerability and Risk Management (VRM) Team is aware of recently disclosed vulnerabilities in Samba.

Technical Details

- **Out-of-bounds read vulnerability**
  Due to insufficient length checks in winbindd_pam_auth_crap.c. When performing NTLM authentication, the client replies to cryptographic challenges back to the server. These replies have variable lengths, and Winbind fails to check the lan manager response length. When Winbind is used for NTLM authentication, a maliciously crafted request can trigger an out-of-bounds read in Winbind, possibly resulting in a crash. CVE-2022-2127

- **Infinite loop vulnerability**
  Found in Samba's mdssvc RPC service for Spotlight. When parsing Spotlight mdssvc RPC packets sent by the client, the core unmarshalling function sl_unpack_loop() did not validate a field in the network packet that contains the count of elements in an array-like structure. By passing 0 as the count value, the attacked function will run in an endless loop consuming 100% CPU. This flaw allows an attacker to issue a malformed RPC request, triggering an infinite loop, resulting in a denial-of-service condition. CVE-2023-34966

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

- CVE-2022-2127, CVE-2023-34966
- https://access.redhat.com/security/cve/CVE-2022-2127
- https://bugzilla.redhat.com/show_bug.cgi?id=2222791
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/BPCSGND7LO467AJGR5DYBGZLTCGTOBCC/
- https://lists.fedoraproject.org/archives/list/package-announce@lists.fedoraproject.org/message/OT74M42E6C36W7PQVY3OS4ZM7DVYB64Z/
- https://security.netapp.com/advisory/ntap-20230731-0010/
- https://www.samba.org/samba/security/CVE-2022-2127.html

- https://access.redhat.com/security/cve/CVE-2023-34966
- https://bugzilla.redhat.com/show_bug.cgi?id=2222793
- https://www.samba.org/samba/security/CVE-2023-34966