



## Bug 2433121 (CVE-2026-0966) - CVE-2026-0966 libssh: Buffer underflow in ssh\_get\_hexa() on invalid input

**Keywords:**

**Reported:** 2026-01-26 23:21 UTC by OSIDB Bzimport

**Status:** NEW

**Modified:** 2026-02-26 01:29 UTC ([History](#))

**Alias:** CVE-2026-0966

**CC List:** 6 users ([show](#))

**Product:** Security Response

**Fixed In Version:**

**Component:** vulnerability

**Clone Of:**

**Environment:**

**Version:** unspecified

**Last Closed:**

**Embargoed:**

**Hardware:** All

**OS:** Linux

**Priority:** medium

**Severity:** medium

**Target Milestone:** ---

**Assignee:** Product Security DevOps Team

**QA Contact:**

**Docs Contact:**

**URL:**

**Whiteboard:**

**Depends On:** [2442912](#) [2442913](#)

**Blocks:**

**TreeView+** [depends on](#) / [blocked](#)

**Attachments** ([Terms of Use](#))

OSIDB Bzimport 2026-01-26 23:21:47 UTC

[Description](#)

The API function `ssh_get_hexa()` is vulnerable, when 0-length input is provided to this function. This function is used internally in `ssh_get_fingerprint_hash()` and `ssh_print_hexa()` (deprecated), which is vulnerable to the same input (length is provided by the calling application).

The function is also used internally in the gssapi code for logging the OIDs received by the server during GSSAPI authentication. This

could be triggered remotely, when the server allows GSSAPI authentication and logging verbosity is set at least to SSH\_LOG\_PACKET (3). This could cause self-DoS of the per-connection daemon process.

---

**Note**

You need to [log in](#) before you can comment on or make changes to this bug.

