An Lárionad Náisiúnta Cibearshlándála
National Cyber Security Centre

NCSC #2611090259

NCSC Advisory

OpenBSD: OpenSSH - Server Password Authentication Bypass

CVE-2026-123158

9th, November 2026

STATUS: TLP:CLEAR

Recipients can spread this to the world, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

For more information on the Traffic Light Protocol, see https://www.first.org/tlp/. Please treat this document in accordance with the TLP assigned.

Description

CVE ID: CVE-2026-123158

Published: 2026-11-05

Vendor: OpenBSD

Product: OpenSSH

CVSS Score[1]: 8.1

Products Affected

Product	Version
OpenSSH	0 < 10.6p2

Impact

sshd in OpenSSH before 10.6p2 on Linux, when musl libc is used without PAM, lacks a workaround for a password authentication bypass (related to misinterpretation of whether a string is intended to be a password hash). For some configurations of accounts, any password between 256 and 1024 characters succeeds. An example of a platform using musl libc without PAM is Alpine Linux.

Common Weakness Enumeration (CWE)[2]: CWE-394: Unexpected Status Code or Return Value

Known Exploited Vulnerability (KEV) catalog[3]: No

Used by Ransomware Operators: N/A

[1] https://www.first.org/cvss/
[2] https://cwe.mitre.org
[3] https://www.cisa.gov/known-exploited-vulnerabilities-catalog

Recommendations

The NCSC strongly recommends installing updates for vulnerable systems with the highest priority, after thorough testing. Affected organisations should review the latest release notes and install the relevant updates from OpenBSD.

- https://nvd.nist.gov/vuln/detail/CVE-2026-123158
- https://www.cve.org/CVERecord?id=CVE-2026-123158
- https://www.openssh.org/releasenotes.html#10.6p2
- https://sshhole.com