contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

OpenBSD OpenSSH exploited

CVE-2026-123158 · on CISA's exploited list since 9 November 2026

Analysis Report

Act today if you run SSH on Alpine Linux or another musl libc host without PAM; the vendor says switch off SSH password authentication at once, then update to OpenSSH 10.6p2. If every SSH server uses …

PREPARED BY	NamiQ	DATE	12 November 2026
FACTS AS OF	12 November 2026	VERSION	1.0
SEVERITY	**High: CVSS 3.1 8.1**	STATUS	On CISA's exploited list; due 12 November 2026

NamiQ © 2026 NamiQ. All rights reserved. This document is the property of NamiQ. It may be shared unaltered, with attribution.
Companion article: namiq.io/insights/openbsd-openssh-cve-2026-123158

The bottom line

> *Act today if you run SSH on Alpine Linux or another musl libc host without PAM; the vendor says switch off SSH password authentication at once, then update to OpenSSH 10.6p2. If every SSH server uses glibc or PAM, you are not affected and can stop.*

At a glance

Fact	Detail
Product	OpenBSD OpenSSH (CVE-2026-123158)
Severity	High: 8.1 (CVSS 3.1)
CISA	On its exploited list since 9 November 2026. Deadline for US federal agencies: 12 November 2026.
Chance of exploitation (EPSS)	0.19, the estimated chance in the next 30 days, as at 12 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	OpenSSH 10.6p2 (released 5 November 2026).
Who looks first	Anyone running an SSH server on a Linux host built with musl libc and without PAM; Alpine Linux is the named example. Glibc systems, hosts using PAM for password authentication, and non-Linux systems are not affected.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run an SSH server (sshd) on any Linux host?	Nothing to do for this CVE.	Check whether it uses musl libc without PAM.
Is that host built with musl libc without PAM, such as Alpine Linux?	Not affected; nothing to do.	Check the OpenSSH version.
Is OpenSSH older than 10.6p2 on that host?	You are on the fixed release.	Disable SSH password login now, then update.
Is password authentication enabled on that host?	The bypass path is closed; still update.	Turn it off at once, then patch.

What it is

On these systems sshd can misread a long string as a valid password hash. The record says that for some account setups any password between 256 and 1024 characters is accepted, letting someone log in without knowing the real password.

Why it matters

The flaw gives an unauthenticated login on an exposed SSH service, which is the front door to a host. It works only on Linux built with musl libc and without PAM, so most estates are untouched; but where it applies, an over-long password walks straight in. Our reading is that the narrow condition is why the score is not higher, yet on an affected host reachable over the network no valid credential is needed, which makes it serious. The vendor says the root cause sits outside OpenSSH, so other software on the same libc may deserve a look.

What the vendor's advisory says

We read two pages on news.ycombinator.com and marc.info. In short:

- The vendor's release announcement says 10.6p2 ships a workaround for the flaw and was put out urgently, a day after the project learned of it, on 5 November 2026.
- It says operators of musl libc Linux without PAM, such as Alpine, should set password authentication off or disable SSH immediately as an interim step.
- It states the issue does not exist on non-Linux systems, on Linux with glibc, or on Linux systems that use PAM for password authentication.
- It says the project considers the root cause to lie outside OpenSSH, but it was well placed to deliver a mitigation quickly.

Things people will get wrong

- We run Linux, so we must be exploitable. Only Linux built with musl libc and without PAM is affected. The record says glibc systems and those using PAM are not.
- It is an OpenSSH bug, so we must update OpenSSH everywhere. The vendor says the root cause is outside OpenSSH; 10.6p2 adds a workaround. Only musl-without-PAM Linux needs it.
- Turning off password login is enough, no update needed. That closes the path now, but the record's fix is OpenSSH 10.6p2; apply it when you can.

How we would triage it

This is our judgement.

The commands only read: they print a version or list what is installed. They come from general knowledge of this kind of product, not from the sources, so check them against the vendor's page

before you run them. Words in capitals are for you to fill in.

Step 1: Find where you run SSH and on what

- List your Linux SSH servers and check which use musl libc without PAM; Alpine Linux is the named example and the only kind at risk.
- Note the OpenSSH version on each.

```
ssh -V
ldd --version
cat /etc/os-release
```

Step 2: Close the exposure now

- On any affected host, turn SSH password authentication off as the vendor advises, or disable SSH, until it is patched.
- Do this first where the host faces the internet.

Step 3: Update to the fixed release

- Update OpenSSH to 10.6p2 on affected hosts, which adds the missing workaround.
- Confirm the running version afterwards.

Step 4: Confirm the setting and version

- Check password authentication is off where you set it, and that OpenSSH is 10.6p2 or later.
- Keep written proof of both.

To close it, read the version from the product itself, not from an old inventory, and save the output with the date. If you cannot update today, write down who owns it, the new date, and what limits exposure until then. CISA's wording adds that you should stop using the product if no mitigation is available.

Send this to your IT provider

Copy it, change the names and dates, and send it. It is a draft for you to check, not a template tested with any provider.

> *Hello, we need your help with a security item. CISA has listed CVE-2026-123158 in OpenSSH, with a required action due 12 November 2026. It affects SSH servers on Linux built with musl libc without PAM; Alpine Linux is the named example, while glibc hosts and those using PAM are not affected. Could you tell us whether we run any such host, where, and which OpenSSH version it runs? The fixed release is OpenSSH 10.6p2 (5 November 2026); as an interim step the vendor advises turning off SSH password authentication. Please confirm in writing, by 12 November 2026, the version on each host and that the fix or the workaround is in place. Thank you.*

Signs it was used

An update closes the hole. It does not tell you whether someone used it first. CISA's required action points to its forensic triage requirements (BOD 26-04). Look for:

- Review SSH authentication logs on affected musl-without-PAM hosts for successful password logins, especially at unusual times or from unfamiliar addresses.
- Where logging records it, look for authentication attempts using very long passwords, between 256 and 1024 characters.
- Check for new or unexpected accounts or access following any such successful login.

The weakness behind it

The record classes this as CWE-394 (Unexpected Status Code or Return Value).

Likely ATT&CK mapping

MITRE ATT&CK is a public catalogue of the steps attackers take, from getting in to causing damage. No source has mapped this flaw to it yet, so the steps below are our prediction from what the record says the flaw allows. They are not MITRE's, the vendor's or CISA's, and an attacker may do other things.

Steps an attacker would likely take with this flaw

The step, in plain words	Stage of an attack	Why we think so
Exploit Public-Facing Application (T1190): Breaking in through a service that faces the internet, such as a web server, VPN or login page.	Initial Access: getting in	The record describes an authentication bypass on an SSH service reachable over the network; an attacker would likely exploit that exposed service directly to gain entry without a valid password.

External Remote Services (T1133): Using a remote-access service such as a VPN or remote desktop to get into the network.	Initial Access: getting in	SSH is an external remote service for logging in; the bypass would typically let an attacker use that remote access path without legitimate credentials.

How to use this: ask your IT provider which control or log would show each step, for example whether sign-in attempts from the internet are recorded. If nobody can answer, that is the gap to close first.

MITRE ATT&CK® is a registered trademark of The MITRE Corporation. Technique names are MITRE's.

The sources, in their words

CISA's catalogue entry:

> *OpenBSD OpenSSH on Linux contains an unexpected status code or return value vulnerability that could allow for authentication bypass.*

The CVE record, published by Mitre on 5 November 2026:

> *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.*

Versions of OpenBSD OpenSSH the record lists as affected:

- all versions before 10.6p2

The affected ranges end before 10.6p2. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

CISA's required action:

> *Apply mitigations in accordance with vendor instructions.*

Check your own project

If you build software, you can compare what a project declares with this CVE from a terminal. The tool reads requirements files, package.json, Maven, Gradle, Cargo, CMake and Dockerfile files, runs nothing, and only the CVE id leaves your machine. Naming the CVEs needs no key.

```
lattice-scan project . --cve CVE-2026-123158
```

Each row says in-range, outside-range, undetermined or lead, with the file and line. That is evidence about what a manifest declares, not about what runs, and a person decides. The verdicts, the CSV columns and a pipeline recipe are in the guide.

Check the servers you run

The same id can be checked against a host. Run this on the machine itself, not on the laptop that deploys to it: it reads installed packages (dpkg, rpm or apk), snaps, the hardware (maker, model, firmware), the running container images with their operating system and packages, and the kernel version, compares them on the spot, and only the CVE ids leave the machine; the inventory stays on it, in ~/.lattice-scan. Naming the CVEs needs no key. Do it on each server after a deployment, and again when a new entry lands.

```
lattice-scan --cve CVE-2026-123158
```

A match is a candidate for a person to confirm, not a finding. A distribution can fix a CVE under an unchanged version number, so a match is a candidate; on Debian-family hosts the report also shows whether the package's own changelog names the CVE. By default it opens the images your containers are running and reads their operating system and package list; a deep scan (--deep, a few minutes) opens every local image and the Python, Node, Java and Ruby packages inside them; for what an image declares, use the project check on its Dockerfile.

Guide: namiq.io/lattice/guides/choose-your-channel. MCP server (io.namiq/lattice in the MCP registry): namiq.io/lattice. Package: pypi.org/project/lattice-scan, or namiq.io/apt.

What we do not know yet

- The sources do not say which account configurations accept the over-long password, so which accounts on an affected host are at risk is unclear.
- They do not name the other software on musl libc that may share the root cause the vendor places outside OpenSSH.
- They do not give a way to tell from logs whether a successful login used the bypass.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 12 November 2026; the vendor's advisory wins where it differs.
- The sections headed "The bottom line", "Does this apply to you?", "What it is", "Why it matters", "Exposure by situation", "Things people will get wrong", "Likely ATT&CK mapping", "How we would triage it" and "Send this to your IT provider" are our interpretation of the sources, not a statement by CISA or the vendor.

Appendix 1. Severity decoded

CVE-2026-123158: score 8.1, `CVSS:3.1/AV:N/AC:H/PR:N/UI:N/S:U/C:H/I:H/A:H` As the CVE record gives it. The record's own score can differ from the base score on the NVD record.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	High	Needs conditions outside the attacker's control.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Unchanged	Damage stays inside the vulnerable component.
Confidentiality	High	Total loss of confidentiality.
Integrity	High	Total loss of integrity.
Availability	High	Total loss of availability.

Appendix 2. Timeline

Date	Event
5 November 2026	CVE record published by Mitre.
9 November 2026	CISA added it to its list of exploited vulnerabilities.
12 November 2026	CISA's deadline for US federal agencies.

Appendix 3. Exposure by situation

These priorities are our judgement from the attacker prerequisites in the sources. They are not vendor ratings.

Your situation	Priority	Timeframe
An Alpine or musl-libc Linux SSH server without PAM, reachable from the internet, with password login on	High	within CISA's window
An affected musl-libc host without PAM, SSH reachable only on an internal network, password login on	Medium	this week
An affected host where SSH password authentication is already disabled	Low	next patch cycle

SSH servers only on glibc hosts, or hosts using PAM	None	none for this CVE

Appendix 4. Definition of done

- Every OpenBSD OpenSSH you run is listed, with its version.
- Each is outside the affected list, or the vendor's mitigation is in place.
- The version output or a screenshot is saved with the date.
- Your projects' declared dependencies were checked against this CVE, and every row has a written reason.
- Logs for the weeks before the update were searched, and anything odd was written down.
- Anything not done has an owner and a date.

Sources

- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- CVE record for CVE-2026-123158: https://www.cve.org/CVERecord?id=CVE-2026-123158
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Advisory or release notes read: news.ycombinator.com/item: https://news.ycombinator.com/item?id=50377976
- Advisory or release notes read: marc.info: https://marc.info/?l=openssh-unix-dev&m=179388064263131&w=2
- Reference in the CVE record: www.openssh.org: https://www.openssh.org/releasenotes.html#10.6p2
- Reference in the CVE record: github.com: https://github.com/openssh/openssh-portable/commit/4353fdc43ef646c43a8dda7025cc1a898caf1482
- Reference in the CVE record: news.ycombinator.com: https://news.ycombinator.com/item?id=50378228