contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Mitel OpenScape 4000: new CVE

CVE-2026-137721 · record published 27 November 2026

Analysis Report

Anyone running Mitel OpenScape 4000 or OpenScape 4000 Manager on V11 R0.22 through V11 R2.11, or V10 R1.68 and earlier, must upgrade — the score is 10 and the vendor's advisory says no login is …

PREPARED BY	NamiQ	DATE	27 November 2026
FACTS AS OF	27 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 10.0**	STATUS	Not on CISA's exploited list; exploitation not recorded

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/mitel-openscape-4000-cve-2026-137721

The bottom line

> *Anyone running Mitel OpenScape 4000 or OpenScape 4000 Manager on V11 R0.22 through V11 R2.11, or V10 R1.68 and earlier, must upgrade — the score is 10 and the vendor's advisory says no login is needed to exploit it. Check your installed version first.*

At a glance

Fact	Detail
Product	Mitel OpenScape 4000 (CVE-2026-137721)
Severity	Critical: 10 (CVSS 3.1)
Status	A new CVE record, published by Mitre on 27 November 2026. Not on CISA's list of exploited vulnerabilities when we read it on 27 November 2026, which means nothing public says yet that anyone is using it.
Fixed in	V11 R2.14 or later (both products). Hotfix PLT HF5 for V11 R1.26. A Mitel-supplied patch for V10 R0.28 through V11 R0.22 (OpenScape 4000) or V10 R1.34 through V11 R0.22 (Manager).
Who looks first	Any organisation running Mitel OpenScape 4000 (V11 R0.22 through V11 R2.11, or V10 R1.68 and earlier) or OpenScape 4000 Manager (same V11 range, or V10 R1.34 through V10 R1.68).

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Mitel OpenScape 4000 or OpenScape 4000 Manager?	Nothing to do for this CVE.	Check which version is installed.
Is the installed version V11 R0.22 through V11 R2.11, or V10 R1.68 or earlier?	Nothing to do for this CVE.	This version is affected — check network access next.
Can an untrusted user reach the Platform component over the network?	Still patch; a score-10, no-login flaw warrants it regardless of exposure.	Treat as highest priority; restrict access and patch immediately.

What it is

The Platform component of OpenScape 4000 and its Manager does not properly sanitise input parameters, allowing an attacker to inject operating-system commands and run them on the system.

The vendor's advisory says no login is needed to trigger this.

Why it matters

A score of 10 is the maximum. The vendor's advisory says MTLVULN-1786 can be triggered by an unauthenticated attacker, so network reachability alone is enough — no stolen credential is needed. Command injection (CWE-78) means the attacker runs arbitrary operating-system commands on the telephony platform, not merely reads data. Our reading is that a PBX or management platform reachable beyond its own local segment should be treated as the highest-priority fix; unauthenticated command injection on a management component is the worst combination of access and impact.

What the vendor's advisory says

We read one page on www.mitel.com. In short:

- Advisory MISA-2026-0013 (18 November 2026) also covers MTLVULN-1785 (unauthorized access, improper authentication, unauthenticated, rated critical) and MTLVULN-1793 (command injection from an adjacent network, unauthenticated, rated critical).
- The vendor says to upgrade to V11 R2.14 or later, apply PLT HF5 for V11 R1.26, or apply the supplied patch for V10 R0.28 through V11 R0.22 (OpenScape 4000) or V10 R1.34 through V11 R0.22 (Manager).

Things people will get wrong

- Only the desk phones or handsets need attention, not the server software. The CVE record and the vendor's advisory name the OpenScape 4000 and OpenScape 4000 Manager platform software, not individual handsets. The flaw is in the Platform component of the management layer.
- V10 versions are too old to still matter. The CVE record explicitly names V10 R1.68 and earlier as affected. The vendor's advisory confirms V10 versions require a patch or upgrade.
- A strong admin password makes this unexploitable. The vendor's advisory says MTLVULN-1786 can be exploited by an unauthenticated attacker. No login is needed; credentials do not block this flaw.

How we would triage it

This is our judgement.

Step 1: Find the versions you run

- Check the administrative console or system information screen of OpenScape 4000 and OpenScape 4000 Manager to confirm the installed release number.
- Compare against the affected ranges: V11 R0.22 through V11 R2.11, or V10 R1.68 and earlier for OpenScape 4000; the same V11 range or V10 R1.34 through V10 R1.68 for Manager.

Step 2: Check and reduce network exposure

- Identify whether the Platform component is reachable from the internet or from network segments that include untrusted hosts.
- If it is, restrict access at the firewall level until the upgrade is in place — the vendor's advisory says no login is needed to trigger the flaw, so network reachability is the main risk factor.

Step 3: Apply the vendor's fix

- Upgrade to V11 R2.14 or later if on the V11 branch; apply hotfix PLT HF5 if running V11 R1.26 as a minimum step.
- If running V10 R0.28 through V11 R0.22 (OpenScape 4000) or V10 R1.34 through V11 R0.22 (Manager), apply the Mitel-supplied patch described in advisory MISA-2026-0013.

Step 4: Confirm the fix is in place

- After the upgrade or patch, verify the installed version shows V11 R2.14 or later, or confirm the hotfix or patch reference from the advisory is listed as applied.
- Record the version and the fix confirmation in writing so you have evidence for any audit or follow-up enquiry.

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.

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.

> *We are reviewing CVE-2026-137721, a command injection vulnerability in Mitel OpenScape 4000 and OpenScape 4000 Manager with a CVSS score of 10. The affected versions are V11 R0.22 through V11 R2.11 and V10 R1.68 and earlier. The vendor's fix is V11 R2.14 or later (advisory MISA-2026-0013, 18 November 2026). Please confirm whether we run either product, which exact version is installed, and whether the upgrade or patch has been applied or is scheduled. We would like written confirmation of the installed version and fix status by [date].*

The weakness behind it

The record classes this as CWE-78.

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	CWE-78 on a network-accessible management component, exploitable without authentication per the vendor's advisory, would likely be the route an attacker uses to gain initial access to the system.
Command and Scripting Interpreter (T1059): Running commands or scripts on a machine, such as a shell or PowerShell.	Execution: running the attacker's code	CWE-78 is OS command injection; a successful exploit would likely invoke a shell on the host, giving arbitrary command execution — the record confirms commands run within the system context.

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

The CVE record:

> *A vulnerability in the Platform component of Mitel OpenScape 4000 and OpenScape 4000 Manager could allow an attacker to conduct a command injection attack due to insufficient parameter sanitization. A successful exploit could allow an attacker to execute arbitrary commands within the context of the system. This vulnerability affects OpenScape 4000, versions V11 R0.22 through V11 R2.11 and V10 R1.68 and earlier, and OpenScape 4000 Manager, versions V11 R0.22 through V11 R2.11 and V10 R1.34 through V10 R1.68. This is MTLVULN-1786.*

Versions of Mitel OpenScape 4000 the record lists as affected:

- V11 R0.22 up to, but not including, V11 R2.14

The record gives no version ranges. Use the vendor's advisory for the affected versions.

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-2026-137721
```

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-2026-137721
```

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 whether any network path to the Platform component is sufficient or whether it must be directly internet-exposed for the flaw to be reachable.
- The sources do not name the specific parameter or input field that lacks sanitisation, so it is not clear whether a configuration change could limit exposure without a full upgrade.
- The advisory does not list a fix for V10 versions earlier than V10 R0.28; it is not stated whether those versions are end-of-support with no patch available or whether one will follow.
- Exploitation is not recorded. That is not the same as none.
- This is a new record: scores, versions and wording can change in the first days, and they are as at 27 November 2026. We read the vendor pages listed under Sources; nothing here has been tested.
- 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-2026-137721: score 10, `CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H` As the CVE record gives it.

Metric	Value	What it means here
Attack vector	Network	Reachable over a network, with no need to be on the same segment.
Attack complexity	Low	No special conditions beyond the flaw itself.
Privileges required	None	No account is needed.
User interaction	None	No one has to do anything.
Scope	Changed	Damage reaches beyond 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
27 November 2026	CVE record published by Mitre.

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
Running an affected version with the Platform component reachable from the internet or an untrusted network	High	This week
Running an affected version and unable to confirm the Platform component is isolated from untrusted hosts	High	This week
Running an affected version with the Platform strictly isolated to a small set of trusted administrators	Medium	Next scheduled patch cycle, with urgency
Running V11 R2.14 or later on both products	None	None for this CVE

Appendix 4. Definition of done

- Every Mitel OpenScape 4000 you run is listed, with its version.
- Each is outside the affected list, or the vendor's fix or mitigation is in place.
- The version output or a screenshot is saved with the date.
- Anything not done has an owner and a date.

Sources

- CVE record for CVE-2026-137721: https://www.cve.org/CVERecord?id=CVE-2026-137721
- CISA Known Exploited Vulnerabilities catalogue: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- Advisory or release notes read: www.mitel.com/support/security-advisories/mitel-product-secur: https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-misa-2026-0013