contact@namiq.io · namiq.io

NamiQ

SECURITY ADVISORY

Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router exploited

CVE-2026-103406 · on CISA's exploited list since 25 November 2026

Analysis Report

PREPARED BY	NamiQ	DATE	26 November 2026
FACTS AS OF	26 November 2026	VERSION	1.0
SEVERITY	**Critical: CVSS 3.1 9.8**	STATUS	On CISA's exploited list; due 28 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/hewlett-packard-enterprise-hpe-juniper-cve-2026-103406

The bottom line

> *Anyone running Juniper Session Smart Conductor on an affected version must act by 28 November 2026. Find the Conductor version immediately and upgrade to 7.0.5, 7.1.7, or 7.2.3.*

At a glance

Fact	Detail
Product	Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router (CVE-2026-103406)
Severity	Critical: 9.8 (CVSS 3.1)
CISA	On its exploited list since 25 November 2026. Deadline for US federal agencies: 28 November 2026.
Chance of exploitation (EPSS)	0.02, the estimated chance in the next 30 days, as at 26 November 2026
Ransomware use	Not recorded by CISA. That is not the same as none.
Fixed in	Session Smart Conductor 7.0.5, 7.1.7, and 7.2.3 and all subsequent releases, per the record published 28 October 2026. No vendor advisory page was available to confirm further detail.
Who looks first	Operators of Juniper Session Smart Conductor running any version before 7.0.5, any 7.1.x before 7.1.7, or any 7.2.x before 7.2.3. CISA also names Session Smart Router, but the CVE record does not list it as an affected product.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run Juniper Session Smart Conductor anywhere?	Nothing to do for this CVE.	Check the version running (next question).
Is the Conductor on a version before 7.0.5, before 7.1.7 (on a 7.1.x line), or before 7.2.3 (on a 7.2.x line)?	No action needed; you are on a fixed release.	Patch or restrict access; see next question for urgency.
Can untrusted systems or the internet reach the Conductor's provisioning interface?	Patch urgently but within your normal change window.	Restrict access immediately and patch the same day.

What it is

A remote attacker can send a specially crafted salt minion ID to the AutomatedProvisioner component and have arbitrary OS commands run as root on the Conductor. The record names no authentication condition.

Why it matters

The record scores this 9.8 (CVSS 3.1). The description states no authentication condition, meaning any system able to reach the provisioner could send a crafted salt minion ID. CWE-78 at this severity lets an attacker pivot from one malformed input to full root control in a single step. Our reading is that the three-day CISA window reflects how directly exploitable unauthenticated remote root execution is, though the record does not state that exploitation has been confirmed.

Things people will get wrong

- Session Smart Router is confirmed vulnerable by this CVE record. CISA names both Conductor and Router in its listing, but the CVE record names only Session Smart Conductor as the affected product. Do not treat the Router as confirmed affected from the record alone.
- A firewall in front of the Conductor removes the need to patch urgently. Network restriction lowers exposure but does not remove the flaw. The CISA deadline applies regardless of network position, and internal hosts or compromised devices could still reach the provisioner.

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 the Conductor version you run

- Log in to each Session Smart Conductor instance and note its software version.

```
show system version
```

Step 2: Restrict access to the provisioning interface

- Confirm the AutomatedProvisioner interface is not reachable from untrusted networks or the internet.

- If it is reachable, apply firewall or ACL rules to limit access to known management hosts before patching is complete.

Step 3: Upgrade to a fixed release

- The record names 7.0.5, 7.1.7, and 7.2.3 as the fixed releases for each active version line.
- Follow HPE Juniper's standard upgrade procedure for Session Smart Conductor to reach the appropriate fixed version.

Step 4: Review for signs of exploitation if the device was exposed

- Check Conductor logs for unexpected root-level process executions not initiated by a known operator action.
- Look for new or altered OS-level accounts, changed authorised keys, and unusual outbound connections from the Conductor host.

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.

> *We are writing regarding CVE-2026-103406, an OS command injection flaw in Juniper Session Smart Conductor scored 9.8 (CVSS 3.1). It allows a remote attacker to execute arbitrary commands as root via a crafted salt minion ID in the AutomatedProvisioner. CISA has added this to its known-exploited catalogue with a remediation deadline of 28 November 2026. The record names fixed versions as Conductor 7.0.5, 7.1.7, and 7.2.3. Please confirm in writing whether we run Session Smart Conductor, which version is installed, whether the provisioning interface is internet-facing, and that the upgrade to a fixed release has been completed or is scheduled. We would like written confirmation by 27 November 2026.*

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:

- Unexpected root-level process executions on the Conductor host that do not correspond to operator activity recorded in the provisioning logs.

- New or altered OS-level accounts, changed sudoers entries, or SSH authorised keys added during the period of potential exposure.
- Unusual outbound network connections from the Conductor, particularly to hosts outside the management network.

The weakness behind it

The record classes this as CWE-78 (Improper Neutralization of Special Elements used in an OS Command).

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 AutomatedProvisioner is a network-reachable component; a remote attacker would likely exploit it as a public-facing application to gain initial entry, as the record describes no authentication barrier.
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 OS command injection would typically result in commands passed to and executed by a system shell interpreter, matching the record's description of arbitrary command execution as root.
Create Account (T1136): Creating a new account so the attacker can come back later.	Persistence: staying in	With unrestricted root command execution gained via the injection, an attacker would likely create a persistent account on the Conductor as a follow-on step to maintain access.

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:

> *Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router contain an OS command injection vulnerability that could allow a remote attacker to execute arbitrary commands as root via a specially crafted salt minion ID.*

The CVE record, published by Juniper on 28 October 2026:

> *An Improper Neutralization of Special Elements used in an OS Command vulnerability in the AutomatedProvisioner in Juniper Networks Session Smart Conductor allows a remote attacker to execute arbitrary commands as root via a specially crafted salt minion ID.*

Versions of Juniper Networks Session Smart Conductor the record lists as affected:

- all versions before 7.0.5
- 7.1.0 up to, but not including, 7.1.7
- 7.2.0 up to, but not including, 7.2.3

The affected ranges end before 7.0.5, 7.1.7, 7.2.3. Those are the first versions the record does not list as affected; confirm them in the vendor's advisory.

What the record says to do about it, in the vendor's words:

> *The following software releases of Session Smart Conductor have been updated to resolve these specific issues: • 7.0.5 and all subsequent releases; • 7.1.7 and all subsequent releases; • 7.2.3 and all subsequent releases.*

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-2026-103406
```

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-2026-103406
```

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

- Whether authentication is required before a salt minion ID is accepted by the provisioner; the record does not state any authentication condition.
- Whether Session Smart Router is independently affected; CISA lists it alongside Conductor but the CVE record names only Conductor as an affected product.
- Whether any workaround short of patching exists; no vendor advisory page was available to check.
- Whether the provisioning interface is exposed by default or requires explicit configuration to be network-reachable.
- We have not tested this against any environment. Versions and scores are as the sources state them and as at 26 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-2026-103406: score 9.8, `CVSS:3.1/AV:N/AC:L/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	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	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
28 October 2026	CVE record published by Juniper.
25 November 2026	CISA added it to its list of exploited vulnerabilities.
28 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
Conductor on an affected version with the provisioning interface reachable from untrusted networks	High	By 28 November 2026 (CISA deadline)
Conductor on an affected version, provisioning interface restricted to a management network only	Medium	This week
Session Smart Router in use but no Conductor deployed	Low	Confirm with the vendor; the record does not list Router as affected

Conductor already on 7.0.5, 7.1.7, 7.2.3 or later	None	No action needed for this CVE

Appendix 4. Definition of done

- Every Hewlett Packard Enterprise (HPE) Juniper Session Smart Conductor and Session Smart Router 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-2026-103406: https://www.cve.org/CVERecord?id=CVE-2026-103406
- FIRST: Exploit Prediction Scoring System: https://www.first.org/epss/
- Reference in the CVE record: supportportal.juniper.net: https://supportportal.juniper.net/JSA112183