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

> *Organisations that do not run HPE Juniper Session Smart Conductor need take no action here. Those that do run it on an affected version must patch by 28 November 2026; confirm the installed version first.*

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)	0.01, 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, per the record published 28 October 2026.
Who looks first	Teams running HPE Juniper Session Smart Conductor at any version below 7.0.5, from 7.1.0 below 7.1.7, or from 7.2.0 below 7.2.3. CISA also names Session Smart Router; the CVE record does not list it with version ranges.

Does this apply to you?

Answer in order. Stop at the first no.

Question	If no	If yes
Do you run HPE Juniper Session Smart Conductor?	Nothing to do for this CVE.	Check the installed version.
Can untrusted systems reach the Conductor's AutomatedProvisioner?	Exposure is reduced; patching is still required.	Treat this as the highest priority and patch before the deadline.

What it is

An attacker who can send a specially crafted salt minion ID to the AutomatedProvisioner can run arbitrary operating system commands as root on the Conductor, with no authentication required. The record scores this 9.8 on CVSS 3.1.

Why it matters

A CVSS 9.8 command injection granting root access with no authentication gives an attacker full control of the Conductor. Any system that can reach the AutomatedProvisioner can deliver the payload via the salt minion ID. The EPSS of 0.0086 was set before exploitation was confirmed and does not reflect current risk. CISA names Session Smart Router alongside Conductor, but the CVE record lists only Conductor with specific version ranges. Our reading is that Router users should seek HPE Juniper guidance directly, as the record gives no affected or fixed versions for it.

Things people will get wrong

- The low EPSS score means exploitation is unlikely. EPSS reflects probability before exploitation was confirmed. CISA has since added this CVE to its known-exploited catalogue, and the EPSS figure does not capture that change.
- Session Smart Router is affected on the same version ranges as Conductor. CISA names both products, but the CVE record lists only Session Smart Conductor with specific version ranges and fixes. The record does not state affected or fixed versions for the Router.
- Keeping the AutomatedProvisioner off the internet removes the risk. The record describes a remote attacker but does not restrict this to internet access. An attacker already on an internal network could also reach the Conductor.

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 version of Session Smart Conductor you run

- Log in to the Conductor and check the software version. The record names three affected ranges: 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.

```
show system version
```

Step 2: Limit access to the AutomatedProvisioner if patching is delayed

- The record does not name a workaround. The flaw is in the AutomatedProvisioner; until a patch is applied, review whether this component must accept connections from every system on the network.

Step 3: Apply the patched release for your version line

- The record confirms fixes in 7.0.5, 7.1.7, and 7.2.3. Apply the release that matches your current version line and confirm the installed version after the upgrade.
- If you also run Session Smart Router, the record does not list fixed versions for it; contact HPE Juniper for guidance.

Step 4: Review logs for unexpected salt minion activity

- Check Conductor and SaltStack logs for salt minion registration attempts or connections from unexpected source addresses, particularly around and before 25 November 2026.

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 about CVE-2026-103406, an OS command injection flaw in HPE Juniper Session Smart Conductor scored 9.8 (CVSS 3.1). CISA listed it on 25 November 2026 with a deadline of 28 November 2026. Please confirm whether we run Session Smart Conductor and, if so, which version. The affected versions are all releases before 7.0.5, 7.1.0 to below 7.1.7, and 7.2.0 to below 7.2.3. Fixed releases are 7.0.5, 7.1.7, and 7.2.3. Please also check whether we run Session Smart Router — CISA names it, but the CVE record gives no version ranges or fixes for it. Please confirm in writing the installed version and whether the patch is in place by 28 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:

- Salt minion registration attempts or connections from unexpected source addresses in AutomatedProvisioner or SaltStack logs.
- Unexpected root-level process executions or new accounts on the Conductor around or before 25 November 2026.

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 flaw is in a remotely reachable provisioning component; a crafted minion ID is the payload, making initial access via an exposed network service likely.
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 execute arbitrary commands through the system's command interpreter, run as root on the Conductor.

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 Session Smart Router is affected and, if so, which versions are fixed — CISA lists it but the CVE record does not give version ranges or fixes for it.
- Whether the AutomatedProvisioner is reachable from untrusted systems by default or only after specific configuration.
- Whether any workaround short of patching exists — no vendor advisory page could be read.
- 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 AutomatedProvisioner reachable from untrusted networks	High	Before 28 November 2026
Conductor on an affected version on an internal network only	High	Before 28 November 2026
Session Smart Router in use — affected versions and fix not stated in the record	Medium	Seek HPE Juniper guidance this week

Conductor already on 7.0.5, 7.1.7, 7.2.3 or a later release	None	Confirm version and record it

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