Juniper Session Smart Conductor flaw CVE-2026-103406 now exploited; patch available



Juniper and CISA report active exploitation of CVE-2026-103406 (CVSS 9.8), a root-level command injection flaw in Session Smart Conductor. A fix has been available since October 28.

- CVE-2026-103406 is a remotely exploitable OS command injection flaw with a CVSS score of 9.8.
- It affects the AutomatedProvisioner service and allows arbitrary commands with root privileges via a crafted Salt minion ID.
- Juniper updated its advisory to say at least one malicious exploitation was reported to its SIRT.
- CISA added the flaw to its KEV catalog; fixed versions are 7.2.3, 7.1.7 and 7.0.5.
- The patch was released on October 28 alongside 17 other fixes in Session Smart Router and Conductor.

Juniper Networks and the US agency CISA have warned that attackers are exploiting a critical vulnerability in Session Smart Conductor, the centralized management and policy platform used to orchestrate Session Smart Routers.

What is affected

The flaw, tracked as **CVE-2026-103406** (CVSS 9.8), is an OS command injection issue in the AutomatedProvisioner service. A remote attacker can use a specially crafted Salt minion ID, the identifier a router presents when registering with the Salt master (the Conductor), to run arbitrary commands with root privileges.

Juniper patched the defect on October 28, together with 17 other vulnerabilities in Session Smart Router and Session Smart Conductor. This week it updated its advisory to mark the flaw as exploited, noting that at least one instance of malicious exploitation had been reported to its SIRT. CISA then added it to its Known Exploited Vulnerabilities catalog.

What to do

Fixed releases are 7.2.3, 7.1.7 and 7.0.5. Juniper urges customers to upgrade as soon as possible and apply mitigations in the meantime. CISA's three-day deadline applies only to US federal civilian agencies, but it advises all organizations to review the KEV list and act on relevant entries.

Because the Conductor manages routers across the network, a compromise at root level could have wide consequences. Institutions running this product should treat the update as urgent and confirm their version status now.

What to do now

1. Identify all Session Smart Conductor and Session Smart Router instances and confirm their versions.
2. Upgrade to a fixed release (7.2.3, 7.1.7 or 7.0.5) as a priority, following emergency change procedures.
3. Apply Juniper's interim mitigations where immediate upgrade is not possible.
4. Review Conductor logs and router registrations for unexpected Salt minion IDs or unusual commands, and escalate any findings to incident response.
5. Add CISA's KEV catalog as an input to your vulnerability management and patch prioritization process.