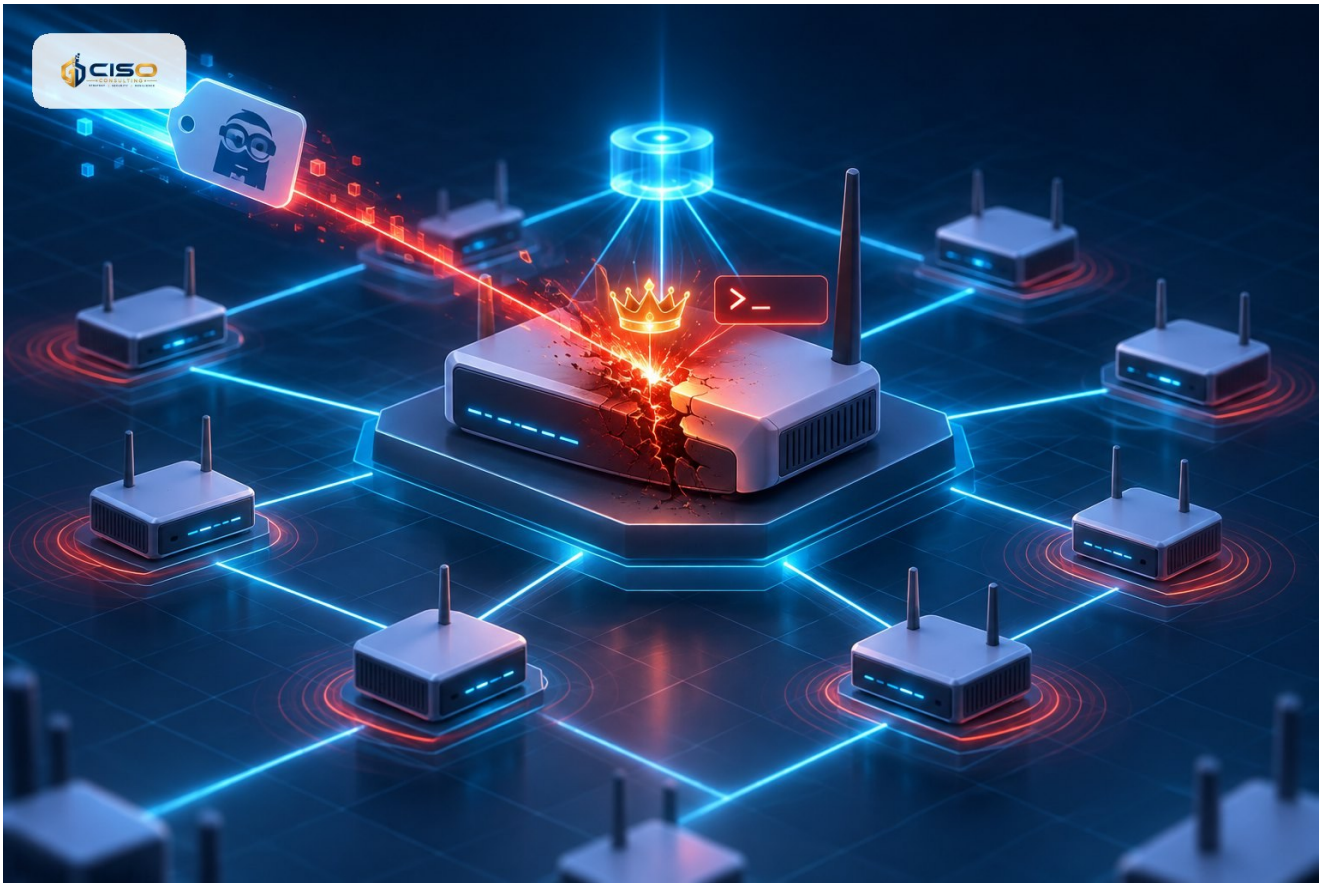
CISA flags OS command injection flaw in HPE Juniper Session Smart Conductor and Router



CISA lists CVE-2026-103406, an OS command injection flaw in HPE Juniper Session Smart Conductor and Session Smart Router that lets a remote attacker run commands as root through a crafted salt minion ID.

- CVE-2026-103406 is an OS command injection vulnerability.
- It affects HPE Juniper Session Smart Conductor and Session Smart Router.
- A remote attacker could execute arbitrary commands as root using a specially crafted salt minion ID.
- CISA requires mitigation per vendor instructions, with a federal due date of 2026-11-28.
- Where mitigations are unavailable, CISA directs discontinuing use of the product.

CISA has added CVE-2026-103406 to its advisory listing. The flaw is an OS command injection vulnerability in HPE Juniper Session Smart Conductor and Session Smart Router.

What the flaw allows

According to the source, a remote attacker could execute arbitrary commands as root by supplying a specially crafted salt minion ID. Root-level execution on a network conductor or router would give an attacker full control of the affected device.

CISA's required action

CISA directs organisations to apply mitigations in line with vendor instructions and to follow its BOD 26-04 guidance on prioritising security updates based on risk, together with its Forensics Triage Requirements. For cloud services, the applicable BOD 26-04 guidance should be followed. If mitigations are not available, the product should no longer be used. Stakeholders are responsible for assessing the internet exposure of each asset. The federal due date is 2026-11-28.

The BOD and due date apply formally to US federal agencies, but the underlying steps are sensible for any institution running these products. The source does not name affected versions or fixed releases, so the vendor's own advisory is the authority on those details.

Practical view

Treat this as a prompt to confirm whether these products exist in your estate, how exposed they are, and whether vendor mitigations have been applied. Do so calmly and in order of exposure, starting with any asset reachable from the internet.

What to do now

1. Inventory all HPE Juniper Session Smart Conductor and Session Smart Router instances.
2. Identify which of these assets are reachable from the internet and prioritise them.
3. Apply the vendor's mitigations as described in the vendor advisory.
4. Perform forensic triage on exposed instances to check for signs of compromise.
5. If no mitigation is available, plan to retire or isolate the affected product.
6. Record the assessment and remediation in your vulnerability management process.