



Executive Summary

CloudWave is issuing this advisory regarding two critical vulnerabilities affecting widely used security infrastructure. One is under active attack and requires immediate action. Please review the sections that apply to your environment and complete the recommended steps.

Advisory 1 — Cisco Identity Services Engine (ISE): Active Exploitation

What's happening

A critical flaw in Cisco ISE and the ISE Passive Identity Connector (ISE-PIC) lets an attacker with no login credentials bypass authentication over the network. A successful attack can give them full root-level control of the device. Cisco has confirmed this is being exploited in real-world attacks, and U.S. CISA has added it to its Known Exploited Vulnerabilities list. (CVE-2026-76460, severity 10.0 of 10.)

Why it matters

ISE controls network access and identity across your environment. An attacker gaining root here could move deeper into your network, and Cisco warns that attackers at this level may erase their own tracks. This is our highest-priority item.

Affected versions and fixes

All ISE and ISE-PIC deployments are affected, regardless of configuration. Update to at least the patched release for your version:

What should you do

1. Patch immediately. Upgrade every ISE and ISE-PIC node to the fixed release above. There is no workaround. Cisco released a broader set of critical patches for ISE and Secure Firewall in the same September update — apply the full update set, not just this single fix.
2. Check for compromise. On each node, review access.log for unexpected usernames. Cisco's detection command is: `show logging application ise-kong/access.log | include dummyuser`. Any output likely indicates malicious activity. In a distributed deployment, check every node.
3. If compromise is found, treat the node as breached — re-image it, restore from a known-good configuration backup, and contact CloudWave immediately.
4. Interim mitigation: until patching is complete, use infrastructure access control lists (iACLs) so only trusted management traffic can reach the device.

Advisory 2 — Check Point Security Management Server

What's happening

A critical flaw in Check Point Security Management Servers and Log Servers could let an attacker without credentials run code as root on the server that controls your firewall policy. There is no evidence of exploitation yet, and no public exploit code exists at this time — but given the severity, prompt patching is strongly recommended. (CVE-2026-91843, severity 9.8 of 10.)



Why it matters

The management server governs your firewall rules and administrator access. A compromise here would undermine a core security control, so we are treating it as urgent even though no attacks have been observed.

Affected versions and fixes

Patch the following via Check Point LivePatch (advisory sk1000155):

- R82.20 — all builds (no hotfix available yet; monitor Check Point and harden per Action 3 below)
- R82.10 — Take 44 or below
- R82 — Take 126 or below
- R81.20 — Take 166 or below
- R81.10 — Take 190 or below
- R81, R80.40, R80.30, R80.20, R80.10, R80 — end of support; a fix is available by opening a Check Point support ticket

This also applies to standalone deployments (management and gateway on one system), Log Servers, and Multi-Domain servers. Check Point's hosted Smart-1 Cloud service is already protected and needs no action.

What should you do

1. Apply the LivePatch fix from Check Point advisory sk1000155 to every Security Management Server and Log Server.
2. Verify — don't assume. If automatic updates are on, confirm the fix actually installed. The command `cplp list` shows installed LivePatches and their status.
3. Harden management access. Confirm the Trusted Clients setting is limited to known, trusted hosts (not "Any IP Address"), and ensure management is never exposed directly to the internet. This closes the path the flaw relies on and is your best protection for R82.20 until a hotfix ships.
4. For end-of-support versions, open a Check Point support ticket to obtain the fix and plan an upgrade to a supported release.