Threat Brief

Updated Sep 21, 2026 - 3:42 AM EDT - askanything-app.com

ACTIVELY EXPLOITED

Orkes Conductor pre-auth RCE exploitation is accelerating, not new but escalating fast

WHAT HAPPENED

Fortinet reports attackers are ramping up exploitation of CVE-2026-58138, an unauthenticated RCE in the Orkes Conductor workflow engine, submitting crafted JavaScript/Python expressions to the workflow API to escape the scripting sandbox and run arbitrary OS commands. Fortinet blocked roughly 7,000 attack attempts in the week of Sept 2-9 alone, a 132% day-over-day jump, with activity concentrated from Germany, Hong Kong, Indonesia, the UAE, and India.

AFFECTED

Orkes Conductor (and Conductor OSS) versions 3.21.21 up to (but not including) 3.30.2 - notably, Conductor OSS ships with authentication disabled by default, and evaluators can be configured with unrestricted host access.

EXPLOITATION

Actively exploited in the wild, confirmed by Fortinet/FortiGuard Labs telemetry; reported by The Hacker News on Sept 19, 2026.

FIX

Fixed in Orkes Conductor 3.30.2 (patched back in June 2026) - upgrade immediately if still on 3.21.21-3.30.1. If you can't upgrade tonight, enable authentication on the workflow API and disable unrestricted host access for script evaluators (restrict `builtin` allowlists to exclude shell/process access).

CHECK IF YOU'RE EXPOSED

Query your Conductor version via its management API/UI; check workflow API access logs for unauthenticated POSTs containing JavaScript/Python expression payloads targeting the evaluator task type.

SOURCE

[The Hacker News - Critical Pre-Auth RCE in Orkes Conductor Workflow Platform Exploited in the Wild](https://thehackernews.com/2026/09/critical-pre-auth-rc e-in-orkes.html) - Sept 19, 2026 - corroborated by [FortiGuard Labs - Orkes Conductor Evaluator RCE Outbreak Alert](https://fortiguard.fortinet.com/outbreak-alert/orkes- conductor-rce)

PATCH AVAILABLE

SolarWinds patches hard-coded key in Access Rights Manager enabling unauthenticated RCE

WHAT HAPPENED

SolarWinds shipped an advisory and patch for CVE-2026-28326 (CVSS 8.8), a hard-coded static cryptographic key baked into Access Rights Manager that an unauthenticated attacker can use to achieve remote code execution. Researcher Kai Huang (Armadin) is credited with the find; SolarWinds has not stated the bug is exploited yet, but hard-coded-key RCEs in identity/access-management tooling are a high-value target the moment technical details circulate.

AFFECTED

SolarWinds Access Rights Manager (ARM) version 2026.2 and all prior versions.

EXPLOITATION

No exploitation observed yet, per SolarWinds; treat as high-priority given the low complexity of hard-coded-key exploitation once reverse-engineered.

FIX

Fixed in ARM 2026.2.1 - upgrade immediately. No workaround exists since the flaw is a hard-coded key in the shipped binary; patching is the only real fix. If you can't patch tonight, restrict network access to the ARM management interface to trusted admin networks only.

CHECK IF YOU'RE EXPOSED

Check your ARM build/version number in the console (Help > About) against 2026.2.1; if below, you're exposed regardless of configuration.

SOURCE

[The Hacker News - SolarWinds Patches ARM Hard-Coded Key Flaw Enabling Unauthenticated RCE](https://thehackernews.com/2026/09/solarwinds-patches-ar m-hard-coded-key.html) - Sept 19, 2026

PUBLIC EXPLOIT

Three CVSS-10 sandbox-escape bugs disclosed in vm2 - widely embedded in Node.js sandboxing and AI-agent code execution

WHAT HAPPENED

Three new CVEs (CVE-2026-93603, CVE-2026-93605, CVE-2026-93606), each CVSS 10.0, were published for vm2, the Node.js sandbox library used to run untrusted JavaScript. The bugs combine a nullish-`this` proxy leak, a `child_process` denylist omission, and a Promise-rejection-sanitizer gap - each independently gives sandboxed code a full escape to host `process` and arbitrary command execution. vm2 still pulls ~800K weekly npm downloads and is a dependency of roughly 900 other packages, including tooling used to sandbox AI-agent code execution.

AFFECTED

vm2 npm package, all versions through 3.12.0.

EXPLOITATION

No confirmed in-the-wild exploitation reported yet; treat as proof-of-concept-private/imminent given the trivial CVSS-10 network/no-auth/no-interaction rating and vm2's use in untrusted-code-execution contexts (including AI agent sandboxes).

FIX

Fixed in vm2 3.12.1 (rolled forward into 3.12.2, released Sept 8, 2026) - upgrade to >=3.12.1. Check exposure with `npm ls vm2` (direct) or `npm ls --all vm2` (transitive); if you can't upgrade immediately and don't need arbitrary host-function exposure, avoid passing non-strict host functions or `child_process`-adjacent builtins into the sandbox context as a stopgap, or pin via `overrides`/`resolutions` to >=3.12.1 for transitive dependents.

CHECK IF YOU'RE EXPOSED

Run `npm ls vm2` and `npm ls --all vm2` in your Node projects, and for AI-agent or code-execution frameworks specifically, check whether they use vm2 (rather than isolated-vm) for isolation.

SOURCE

[VulnCheck - vm2 before 3.12.1 Sandbox Escape RCE via Non-Strict Host Function](https://www.vulncheck.com/advisories/vm2-before-3. 12.1-sandbox-escape-rce-via-non-strict-host-function) - Sept 18, 2026 - corroborated by [Kodem Security - vm2 Sandbox Escape: AI Agent RCE Risk and IOCs](https://www.kodemsecurity.com/resources/vm2-sandbox-es cape-vulnerabilities-the-2026-cve-wave-turning-ai-agents-int o-host-rce-vectors)