6-12 November 2026

Prepared 13 November 2026 | Free edition | Global software relevance

Developments that mattered

Remote administration deserves an explicit owner this week. ScreenConnect activity began on 11 November; ConnectWise's advisory of that date was revised at 18:45 UTC on 12 November. Its assessment concerns independent third-party extensions and unauthorised remote-access clients. Huntress distinguishes actual deployments from attempted reverse spread that it has not seen succeed.

N-central HF2 arrived on 10 November after disclosures on 8 November. Further disclosures and restrictions followed on 12 November. Canada's advisory reports exploitation indications for a specific older CVE; the new Legacy API issue and integration restrictions need a separate scope check. We could not retrieve N-able's dashboard directly and identify the reproduced notice as such.

Wiz's 9 November Qubole research describes AWS access during 14-26 October through customer roles trusting a supplier account, including otherwise unused integrations. Its 11 November update adds an unverified responsibility claim; it does not establish a new attack window or verified attribution.

Potential business impact

For matching environments, remote-management abuse can extend an incident across customer machines. Supplier cloud trust can expose stored information and credentials. Containment or temporary integration restrictions may interrupt support work. These are scope-dependent risks, not a statement that every business is affected.

Affected products, sectors or organisations

Check ScreenConnect environments with the named RMM+ family extensions; N-central hosted or on-premises deployments, their Agents/Probes and relevant integrations; and AWS accounts with Qubole integration roles. Sources establish product and access conditions, not a universal sector exposure. Global software relevance; UK impact not established for these three items.

Questions for the responsible IT/security owner

Do we or our provider match any of those conditions? Which devices, cloud roles, time windows and logs were checked? Are unexplained actions being investigated? What support functions remain restricted? Who can authorise restoration, and what evidence will they require?

Source-supported actions and timeframes

ScreenConnect: verify named extensions are disabled and investigate suspected hosts through separate tools, following the vendor and Huntress response guidance. N-central: confirm Legacy API disabled and follow current vendor restrictions alongside Agent/Probe upgrades. Qubole: remove unused trust; examine CloudTrail from 1 October and, if a role was abused, rotate reachable secrets and revoke active role sessions. Follow each source's conditional instructions. No universal UK deadline is established; agree reporting dates locally.

Decision record for the meeting

Responsible owner: ____ . Evidence of affected scope or no match: ____ . Source-supported action: ____ . Locally agreed reporting date: ____ . Evidence of completion: ____ . Unresolved uncertainty and escalation owner: ____ . Keep this record for each matching service rather than giving a blanket all-clear.

Unresolved uncertainty

ScreenConnect's full scope and initial-access assessment remain under investigation. N-central's separate disclosure claims and evolving restrictions need current vendor confirmation. Missing cloud data-access logs can limit what can be concluded about Qubole-related reads. A source comparison is not an independent forensic examination.

Management meeting takeaway - ColesCyber interpretation

Choose the owner, establish the match and request completion evidence. Ask what could remain accessible after the first containment step. Record uncertainty and a proportionate next reporting date.

Primary evidence and related reporting

ConnectWise: 11-12 Nov

Huntress: SCKit

Canada: 12 Nov

N-able: current dashboard

Wiz: 9 Nov / 11 Nov update

Reproduced N-able notice (dashboard not directly retrieved)

Related ColesCyber reporting

updated ScreenConnect reporting

updated N-central reporting

Qubole investigation checks

AI-assisted research, writing and source comparison; no independent human review claimed.

Prepared 13 November 2026. Dates are source-specific; locally agreed reporting is not a universal deadline.