Ivanti patches two more Connect Secure zero-days chained in attacks



Ivanti has released updates for two further flaws in Connect Secure (ICS) remote access gateways. They were chained in zero-day attacks observed since at least October 1.

- Ivanti has patched two more flaws in Connect Secure (ICS), its remote access gateway.
- The flaws were chained together in zero-day attacks, meaning they were exploited before fixes existed.
- The source dates the attacks to at least October 1.
- The source excerpt does not give CVE numbers, affected versions or victim details.

Ivanti has published security updates for two additional vulnerabilities in Connect Secure (ICS), its remote access gateway. According to BleepingComputer, the flaws were chained in zero-day attacks that have been

under way since at least October 1.

What is known

The two flaws were exploited together, and exploitation began before patches were available. The report describes them as additional to earlier Connect Secure issues. The excerpt available to us does not list CVE identifiers, affected version ranges or the nature of the attacker activity, so those details should be taken from Ivanti's own advisory.

Why it matters

Remote access gateways sit at the network edge and are reachable from the internet, which makes them a frequent target. Because exploitation reportedly dates back to at least October 1, organisations running ICS should consider that a device may have been exposed before it was patched, and not rely on patching alone.

Recommended approach

Confirm whether ICS is deployed anywhere in your environment, including in subsidiaries and with third-party providers. Apply the vendor's updates promptly under emergency change procedures, and review the device for signs of compromise covering the period since early October. Follow Ivanti's guidance for any integrity checks it recommends.

What to do now

1. Inventory all Connect Secure (ICS) appliances, including those run by subsidiaries and third parties.
2. Apply Ivanti's latest updates under an emergency change process.
3. Review logs and run Ivanti's recommended integrity checks for signs of compromise since early October.
4. Rotate credentials and secrets handled by the appliance if compromise is suspected.
5. Report confirmed incidents through your regulator's notification channels, such as the NCA or SAMA where applicable.