News article

May 2024

Sisense Hit by Cyberattack

Business analytics SaaS provider, Sisense, has been hit by a cyberattack, prompting CISA to warn of subsequent attacks.

Max Muir
Information Security Consultant
Email max.muir@waterstons.com

What Happened?

On April 11th, the US Cybersecurity and Infrastructure Security Agency (CISA) released a warning about an attack on Sisense, which provides AI-driven business analytics for over 2,000 organisations worldwide, that could impact Critical National Infrastructure (CNI).

CISA warned organisations using Sisense to reset any credentials used to access the providers' services, as well as any credentials or secrets that could have been exposed to a Sisense service. While more specific details about the attack are unknown, the warning from CISA suggests the incident could be a significant breach, with the potential for further attacks on organisations using the platform.

Wider Implications

Supply chain attacks continue to be one of the most challenging areas of cyber security for organisations. Over the past few years, several major supply chain attacks - such as 3CX and MOVEit - have demonstrated to both organisations and threat actors the widespread impact of a single incident. This continuing rise in supply chain compromises is forcing organisations to focus closely on their security, ensuring suppliers are regularly reviewed against their own standards, as well as monitoring the supplier for cyber incidents that would require a response.

Organisations Should:

- Review if they are using Sisense and if so, follow CISA guidance which includes changing all passwords and any services exposed to it, as well as monitoring for any unusual activity in recent weeks.
- Use a risk-based process to review suppliers; assessing the security posture of the supplier, and the 'secure design' of the solution being procured. This review process should also identify critical dependencies which can be used to inform incident response and business continuity planning.
- Consider reviewing any operational dependencies on SaaS solutions, and ensure contingency planning takes place for the event of an outage or major cyberattack on the supplier.

This article and other fantastic insights are shared in our monthly cyber threat report. You can join the mailing list to receive it here.

Waterstons has 25+ years' experience across the UK and Australia preparing and protection organisations from cyber threats. We are committed to assisting all organisations to stay agile and prepared in today's cyber conscious economy.

Empower your organisation today, get in touch with one of our team members.

info@waterstons.com.au | 02 9160 8430