Iress unauthorised access incident - Client fact sheet 11.30am 17 May 2024

What has occurred?

- On Saturday 13 May 2024 Iress detected and contained an unauthorised accessing of our user space on GitHub.
- Iress uses GitHub to manage software code before it goes live in production on a separate platform.
- As soon as we became aware of the issue, we restricted access to GitHub while commencing a rapid investigation.
- In the course of the investigation, it was discovered that a credential within Iress' GitHub user space was stolen and used to gain access to Iress' OneVue production environment. This production environment is isolated to the (Australian) OneVue businesses.
- The OneVue production environment contains client data and we are investigating the extent and nature of the data accessed.
- Iress has become aware of certain statements made today by the alleged threat actor. The statements made today do not align with the investigations made by Iress to date.
- Investigations have further progressed and at this time we have found no evidence to substantiate the claims made.
- Investigations are ongoing. At this time, there is no evidence that Iress' production environment, software or client data has been compromised beyond what Iress has announced to the ASX.

What is Iress doing to respond?

- Iress has disclosed this incident to the market and relevant authorities. It has also been keeping clients informed through various communications channels and live updates on the Iress Community.
- Iress has now commenced a process of strengthening access and security protocols across all software out of an abundance of caution.

Iress Limited, Level 16, 385 Bourke Street Victoria 3000

What do clients need to do?

- Iress is actively assessing any actions that need to be taken by our clients. If action is required, your relationship manager will let you know.

Questions & Answers

1. Have you reported the incident to authorities? How long did it take you to report it?	The issue was discovered early on Saturday 11 May (AEST) and was reported to the Australian Cyber Security Centre on Monday morning 13 May 2024.
2. Which government agencies / regulatory bodies have been informed?	Iress has engaged with the Australian Cyber Security Centre and relevant authorities about this incident. Iress is actively monitoring our regulatory obligations and will continue working with the relevant authorities and regulators.
3. Who is leading the response to this incident?	A cross-functional internal team with executive oversight is leading the response, supported by third-party expertise as required.
4. Have you engaged specialist third parties to assist with this incident?	Yes, we have engaged third parties including specialist cyber incident and technology experts to support Iress with this incident. We will engage third parties where appropriate to support our ongoing activities in connection with this incident.
5. Has this incident resulted in any disruption to Iress' services to clients?	No, there currently has been no disruption to Iress' services to clients.
6. Has any client data or personal identifying information been accessed as a result of this issue?	Investigations are ongoing. We have provided details about this incident in our ASX announcements. We are not able to provide

	additional details at this time.
7. Is there a chance my software environment has been compromised?	As stated in our ASX announcements, apart from Iress' OneVue production environment, at this time we have found no evidence that the remainder of Iress' production environment, software or client data has otherwise been compromised.
8. Are any other systems compromised?	Investigations are ongoing. We have provided details about this incident in our ASX announcements. We are not able to provide additional details at this time.
9. What remediation steps have you taken?	We have provided details about this incident in our ASX announcements. We are not able to provide additional details at this time.
10. What do clients need to do?	For the majority of clients, no action is required. In some instances, it will be recommended that clients update their security credentials. If this impacts you, your relationship manager will let you know.