Client fact sheet: Completion of internal investigation into unauthorised access incident

2 July 2024

ASX Release 2 July 2024

Iress has concluded its internal investigation into the unauthorised access of Iress' user space on GitHub as first announced on 13 May 2024.

The investigation has found no evidence of unauthorised access to Iress' production environment, software or client data other than a limited portion of Iress' OneVue production environment. This environment primarily contained information of a technical nature such as metadata, blank questionnaires and test files. Within the test files, Iress also identified a limited amount of personal information relating to 20 individuals who were employees of OneVue and its clients, and had entered their personal information for testing purposes. Each of these individuals has been contacted directly about the incident and provided with appropriate guidance and support.

Iress has also engaged specialist cyber incident and forensic technology providers to assist in response to the incident.

As previously announced, Iress is aware of statements made by the alleged threat actor regarding publishing source code taken from Iress' GitHub user space. Iress confirms that it does not rely on the secrecy of its code as a security measure and has continued to take steps to reinforce security controls to protect its software and systems.

Iress has maintained regular service to clients throughout this incident and thanks its clients for their patience and support as we have worked to resolve this matter.

Iress will keep the market informed if there are any further significant developments. The release of this announcement was authorised by the Iress Board.

In the ASX statement released today Iress mentions that its internal investigation is now complete - when will a report be made available?
Iress has engaged specialist cyber incident and forensic technology providers to assist in response to the incident. One output of this support is a client report which will be available shortly.

Is there a timeframe for when this report is expected to be completed?
We expect the report to be available by around the end of July.

What was the nature of the personal information uncovered in the OneVue breach? Was it client data?
The personal information impacted by the incident was identified in test files which included a limited amount of personal information entered by employees for testing purposes. This related to 20 individuals, each of whom have been contacted directly about the incident and provided with appropriate guidance and support.

Our investigations have identified no evidence of unauthorised access to any other client data as a result of the incident.

Is Iress concerned about the fact that its source code may be leaked by the threat actor?
No. Iress does not rely on the secrecy of its code as a security measure and has continued to take steps to reinforce its security controls to protect its software and systems.

What does Iress mean when it says it doesn't rely on the secrecy of its code as a security measure?
Iress has a rigorous and multi-layered approach to protecting its software.

As part of our software lifecycle process, the source code contained in GitHub is in its 'raw' form. After being submitted to GitHub, it goes through a series of checks, changes and amendments as well as passing through a number of systems before ultimately becoming part of our live software.

In addition to this, Iress has a dedicated infosecurity team which employs a wide array of industry-leading protections to further reinforce the security of our software and systems. This includes robust internal and external penetration testing, bug bounty programs and retrospective code reviews.

Were there any secrets contained in GitHub? Have these been rotated?

It is not our standard practice to store credentials within GitHub. However, following the incident, our review determined that there were a number of credentials contained within GitHub. These have all now been rotated and updated.

Can Iress share any indicators of compromise (IOCs)?
Iress has shared these with the Australian Cyber Security Centre.