Public Statement

On 23 January 2024, a vulnerability was detected in our Registry system.

We have conducted an initial forensic review with an independent cyber security partner. This review identified that the vulnerability was due to a misconfiguration in our third party-supplied Registry system, which had been implemented in January 2021.

This vulnerability allowed access to non-public names and addresses. It did not link any individuals to registered entities or roles held.

We immediately took action to resolve the issue and have separately written to certain individuals whose name and address was accessed and to whom we owe an obligation to communicate individually.

We deeply regret this has occurred and are currently undertaking further investigations to determine how this happened.

We have been working throughout with the Jersey Office of the Information Commissioner.

Further details are available on our website at www.jerseyfsc.org. For enquiries, please email query@jerseyfsc.org.

Proactive FAQs (website)

WHAT IS THE TECHNICAL ISSUE

What has happened?

External access to JFSC's online registry is via a web application accessed on the JFSC website. When visitors make registry searches, the web application pulls data from the registry itself. As the registry contains publicly accessible data and restricted data, access controls are in place to limit what can be seen. However, an issue was identified meaning under certain circumstances, it was possible to access restricted data.

On discovery of the issue, a fix was implemented within the hour, and a permanent remedy issued by the software provider was then deployed. This has been validated through testing by our independent cyber security partners.

What exactly was the nature of the vulnerability?

The web application pulls data from the registry via Application Programming Interfaces (APIs). APIs are commonly used as a channel to move data between different applications. When searches are made, the web application and API filter them to ensure access is only provided to publicly available data. When data is returned, the web address, contains a reference to the data record in the registry.

Under certain circumstances, if this reference was changed, the API would not filter the request appropriately and this could return a different record containing restricted data.

Has the JFSC been compromised?

The JFSC's corporate network was not compromised.

What data was accessed?

The information which was accessed was limited to names and addresses, and did not link any individuals to a specific registered entity or any role held.

Is it possible to identify someone's role, or the entity they are connect to, from the information?

No. The names and addresses relate to beneficial owners, controllers, directors, members, nominated persons and company secretaries, and the data accessed does not allow identification of the nature of the role an individual holds.

The information did not link any individuals to a specific registered entity.

The information is held in a single database, and the API is not specific to the role held by an individual. Accordingly it is not possible to identify or guess the role or entity from the data.

MATTERS RELATING TO TIMING

On what date did you first become aware?

23 January 2024.

How long did it take you to fix the issue after discovering it?

An immediate fix was implemented within the hour of our becoming aware of the issue, and a permanent remedy issued by the software provider was then deployed. This has been validated through testing by our independent cyber security partners.

What were your next steps?

We have worked closely with the Jersey Office of the Information Commissioner (JOIC) throughout. Our priority has been our duty of care to those whose data we hold. Before making this public statement we needed to ensure that the vulnerability was permanently fixed in our system, and also that this public statement wouldn't cause harm.

We also conducted a forensic review to ensure we had an accurate picture of what had happened, and to make sure there are no other vulnerabilities in the application that could put data at risk.

Finally, we needed to take steps to notify individuals in line with our legal obligations. Having completed this work, we have issued the public statement today to communicate more broadly and provide transparency.

How long was the vulnerability present in the system?

The system was deployed in January 2021 and the issue was fixed on 23 January 2024.

Why wasn't the issue identified earlier?

The software has been subject to penetration testing (where cyber-security experts attempt to find and exploit vulnerabilities in computer systems to ensure they are safe) using two separate expert cyber security testing providers and it is also subject to a monthly security scan. The system was also tested by the software provider themselves. However, regretfully, due to the nature of the error the testing did not identify the issue.

MATTERS RELATING TO THE PEOPLE WHOSE DATA WAS ACCESSED

If I am impacted what do I need to do?

The vulnerability has been closed and your name and address can no longer be accessed in this way. You don't need to contact us unless you wish to do so. Whilst the information is limited to names and addresses only we understand you may still have concerns, and anyone with further queries can contact us via the dedicated email address query@jerseyfsc.org.

Do I need to reset my password?

No, as no access details have been compromised there is no need to change your username or password.

How many records do you hold, and how many of these have been impacted?

We hold approximately 1 million separate records in our registry system. In many instances, this includes individuals who are listed on multiple occasions due to the numerous roles they hold and different relationships with multiple service providers.

Of these, 66,806 individuals have had their names and addresses accessed via the API in circumstances where this information was not already in the public domain through the registry system.

Of the 66,806, we have directly written to the 2,477 people who we have assessed may be potentially impacted, in accordance with our obligations under the Data Protection (Jersey) Law 2018.

Why have you written to 2,477?

It is important to note that only names and addresses were accessed with no link to any specific registered entity or any role held. We have written directly to those people who we have assessed fall into a higher risk category. We have also communicated more widely with a public statement and provided further information on our website.

How did you determine who is impacted?

In accordance with the Data Protection (Jersey) Law 2018, we undertook a risk assessment following an internationally recognised practice using the framework issued by the European Union Agency for Cyber Security (ENISA), and have communicated according to the outcomes of the risk assessment.

I have not received a letter. How do I know if I have been impacted?

We have written directly to certain people, in line with our legal obligations. However we recognise that individuals may still have concerns, and anyone with specific questions can contact their local service provider or contact us. Information is available on our website at jerseyfsc.org.

If you have not received a letter and have any queries you can contact us via the dedicated email address query@jerseyfsc.org.

Will you be telling service providers if their clients have been impacted?

We will continue to work with service providers, and they will be able to provide more information to their clients directly.

Who accessed the data?

As the data was accessed via a public API, it is unfortunately not possible for us to say who has accessed it with certainty.

Do you know what has happened to the data?

With the support of our independent cyber security partners, we have conducted searches, including on the dark web, to see if there is any evidence that the data has been exposed. We have no evidence of this, and monitoring is ongoing.

ASSURANCE ABOUT OUR SYSTEMS

Are other JFSC systems secure?

We recognise that it is never possible to eliminate all risk. However we also understand that no data compromise is acceptable, and we work hard to ensure controls are in place to protect the information we hold. All JFSC systems and networks are subject to comprehensive risk assessments, and periodic external testing to ensure the security of systems and data. Additionally, our systems are subject to 24/7 security monitoring by a specialist provider.

What further steps are you taking?

We appreciate that you may want further information and we will be updating our website regularly. We will also be updating our regulated industry regularly to assist them in supporting clients who have been impacted.

We are also commissioning a full review of how the issue arose. This will be delivered by an independent third-party provider.