Exclusive: Visa application portal closed following SC Magazine investigation

Davey Winder

July 21, 2015

VFS Global closes visa application portal following SC Magazine investigation. Editable Schengen visa application forms accessed FOUR DAYS after operating company VFS Global said a vulnerability had been fixed.

Visa applications obtained by SCMagazineUK.com, details redacted.

An *SCMagazineUK.com* investigation was able to access the editable Schengen visa application forms of three totally random people, some FOUR DAYS after operating company VFS Global said a vulnerability had been fixed and the system was now secure.

Visit the VFS Global website and it not only celebrates having handled 100 million visa applications but also boasts of being the world's largest outsourcing and technology services specialist for governments and diplomatic missions worldwide. It specialises in "visa and passport issuance-related administrative and non-judgemental tasks" for client governments, of which there are 45 around the world. What you won't find any mention of is what appear to be systemic failures when it comes to security.

A vulnerability which first hit the media courtesy of *SCMagazineUK.com* contributor and veteran security journalist Davey Winder back in 2007, and led to an independent enquiry ordered by the UK Foreign Secretary, has re-emerged last week some eight years on.

According to the European Commission "the border-free Schengen Area cannot function efficiently without a common visa policy which facilitates the entry of legal visitors into the EU, while strengthening internal security" and that is delivered by way of the so-called Schengen Visas that are given for up to three months at a time. So it came as something of a surprise to discover that the company responsible for the administration of these visa applications could potentially be putting that internal security at risk at least as far as one part of that system was concerned.

The Guardian briefly reported how part of the Schengen Visa application system suffered a 'technical glitch' which allowed users to access the applications of complete strangers (also reported by SCMagazine). Actually, that technical glitch was more of a security vulnerability; this was the same vulnerability that VFS Global was first made very aware of back in 2007. The company issued a fix, but as an *SC MagazineUK*investigation can exclusively reveal, this fix was also easily bypassed allowing random application forms to be accessed by using the same basic vulnerability.
We first became aware of the latest security failure in the visa application system when*SCMagazineUK.com* was approached by Alexey Utkin, head of financial practice at technology consultancy DataArt UK. Utkin pointed us in the direction of the *Guardian* story which broke over the weekend, and was concerned that the promised fix had not been properly implemented. Unaware at the time that he was talking to the journalist responsible for breaking the original story back in 2007, Utkin thought we would find the simplicity of the vulnerability unbelievable. He was right, but equally unbelievable was the fact that a system responsible for taking Schengen Visa applications for Italy visa applications submitted in UK could remain so fundamentally broken on the security front as we soon discovered.
"On Wednesday night last week I was trying to access my family Italian visa application forms to print those out before our appointment and realised VFS Global had released a new online visa application system since I originally filled in the forms and hadn't migrated the data, so I had to fill all three applications again" Utkin told *SC*, continuing "while fighting with numerous glitches trying to do this, I realised that the new visa system doesn't secure applications data at all. In its system only the application reference number was required to get access to the application data, and reference numbers were sequential – allowing any user to get anyone else's data."
This immediately rang alarm bells with Winder who recalled his earlier investigation and the words of the UK government investigation report by Linda Costelloe Baker which stated "VFS did not appear to have had a formal security function, and thus an effective security procedure to cover software development and testing. VFS and UKvisas agree that no third party penetration tests were carried out in the development phase of the online system or after it was launched. This is a serious and very basic failing."

Those alarm bells got louder when VFS Global told *The Guardian* "data/information security is an extremely critical element of our service solution. Our systems undergo stringent external independent audits on a periodic basis. Testing and auditing are ongoing processes at VFS Global for which we have dedicated teams..." If this were, indeed, the case then one has to wonder how a beta system for visa applications was allowed to be put into a live environment as VFS says happened with the 'glitch' discovered by Utkin? What's more, one wonders what the form this 'stringent external independent auditing' takes.
SCMagazineUK.com spoke to Mike Woodhead, technical director of penetration testing company CQrity who told us that "releasing a beta version, especially of something so critical as a visa application, goes against all common sense and suggested deployment guidelines. This is not just any data, we're talking about peoples personal details, it's a clear breach of the Data Protection Act" and further "any Security Consultant worth their salt should be able to spot something as basic as a enumeration of an integer value, especially on the URL."

But things got worse, a lot worse, when Utkin revealed that while what he refers to as the "surface manifestation of the problem" was removed by the Thursday, the fix that had been put into place was just as broken. "I immediately managed to spot another way to access any other applicant data without any special tooling" Utkin says "this once again confirms VFS incompetence in the data security matters on multiple layers, matters which should be so central for their business." And Utkin should know, he has worked for many years with DataArt and appreciates the kind of design, testing and security audit practices that should be applied to systems engineering, particularly systems containing such sensitive data as the visa application system.

"I was surprised that VFS didn't apply any of these principles in the new Italian visa system, showing total incompetence in the area of application and data security" Utkin told *SC*, concluding "I can understand software bugs but, from my experience, I am sure that in this case it was a systematic failure throughout. Problems like that wouldn't ever happen if people who designed the system knew the very basics of secure systems architecture or if system has been tested and security audited." Why was Utkin so angry about this? Simple, the fix that VFS Global had put into place was guilty of an almost identical lack of understanding about how good data security works and was still putting his family information at risk. Here's how our investigation managed to access the visa application forms of three totally random people, FOUR DAYS after VFS Global said its system had now been secured. To start with you need to have an open application on the system, which then shows a download button which internally will call a server and download an editable PDF document. As a parameter, this takes a number of the PDF; you guessed it, it is still a sequential number of an application. Worse still, this is then passed with a webpage to a client, and the client can modify it internally in the browser as they see fit. There appears to be absolutely no authentication or permission checks on the server at all. Just alter that sequential numbering and open up any application you like which then becomes editable, by you.

As Mike Woodhead from CQrity says "The concern here is intensified by the fact you can amend the details on the PDF form, allowing a malicious user to potentially ruin someone's life. The deployment of this fix suggests a clear lack of understanding of the original vulnerability..."

SCMagazineUK.com contacted VFS Global with the findings of our investigation, and as a direct result a spokesperson informed us that "We are aware of an issue affecting the site for Italy visa applications submitted in the UK. As a temporary measure we have closed the portal while we implement a new release that resolves the issue. In line with our commitment to information security, we will be carrying out all necessary security checks before the portal is re-launched. VFS Global would like to reassure applicants that information security remains of prime importance to us and we continually evaluate our systems and processes to ensure high service levels."
SCMagazineUK.com also passed our findings onto the offices of the European Data Protection Supervisor and the Information Commissioner's Office in the UK. Back in 2007 the UK Information Commissioner's Office found the Foreign Office in breach of its obligations under the Data Protection Act 1998 and required it to sign a statement of compliance. As a result, visa applications into the UK were taken back under the direct wing of the UK Border Service. Unfortunately, given the historical and current unreliability of VFS Global security measures as they apply to visa applications, it would

seem that some applications are once more being outsourced to the company. A Home Office spokesperson told *The Guardian* that "the UK contract with VFS uses different systems to the system in question… We expect all contractors to comply fully with the UK's stringent data protection requirements."

SCMagazineUK.com expects, for its part, that both the UK and the EU revises its relationship with VFS Global in order to ensure that neither the data privacy of applicants nor the ability to prevent such a dangerous form of identity theft during a time of heightened terrorist alert is ever in doubt again.

Original article — http://www.scmagazineuk.com/exclusive-visa-application-portal-closed-following-sc-magazine-investigation/article/427513/3/