NEWSLETTER
M_SEGURANÇA
Millennium bcp

OUTUBRO 2014 Nº 68

English version

COMO SE PROTEGER DO POODLE

No dia 14 de Outubro foi revelada uma vulnerabilidade num dos protocolos que garantem a segurança das comunicações no acesso a *sites* bancários, designado por protocolo SSL v3.0.

A vulnerabilidade foi apelidada de POODLE (*Padding Oracle On Downgraded Legacy Encryption*) e permite que atacantes cibernéticos obtenham informações criptografadas que, no limite, podem ser os códigos de acesso pessoais (*passwords*).

O SSL v3.0 (*Secure Sockets Layer, version 3*) é utilizado para estabelecer ligações seguras entre os *browsers* dos utilizadores e os servidores dos prestadores de serviços e limita as probabilidades de intrusão e desvio de dados.

Contudo, este protocolo está obsoleto e a maioria dos *browsers* ainda o suporta por forma a garantir a compatibilidade com servidores mais antigos. Criando as condições necessárias para a exploração da vulnerabilidade do SSL v3.0, o atacante cibernético consegue intersetar as comunicações entre o *browser* e o servidor, e forçar o estabelecimento da ligação em SSL v3.0 obtendo, desta forma, as informações dos utilizadores.

Esta vulnerabilidade tanto pode afetar utilizadores que acedem a *sites* bancários através de *browsers* como utilizadores que recorrem a *apps* específicas para o mesmo efeito.

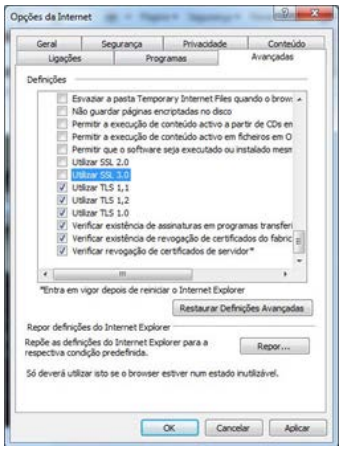
Apesar desta falha de segurança ser de difícil exploração, o Millennium bcp respondeu de uma forma célere à sua resolução e, em menos de 24 horas, desabilitou nos seus servidores a possibilidade de estabelecer ligações com recurso a este protocolo.

O Millennium bcp demonstra assim o compromisso que tem para com a segurança dos utilizadores deste canal, que podem continuar a aceder às suas contas e realizar as suas operações no *site* do Millennium bcp com toda a segurança.

Porque a segurança é uma das prioridades do Millennium bcp, cumpre-nos alertar ativa e preventivamente os nossos Clientes para situações idênticas às acima descritas as quais podem ser consultadas em millenniumbcp.pt, menu M - Tudo sobre: Segurança e, na página seguinte, aceda a "Avisos de Segurança".

Resta-nos identificar algumas medidas que podem ser adotadas para minimizar o risco de um ataque cibernético, variando consoante o *browser* usado, para o Sistema Operativo Windows:

- Para desativar o protocolo SSL v3 no **Internet Explorer® (Windows Vista® ou mais recente),** aceda ao menu **Ferramentas** (*Tools*) > **Opções da Internet** (*Internet Options*) > *tab* **Avançadas** (*Advanced*) e desmarque a opção **Utilizar SSL 3.0** (*Use SSL 3.0)* e **Utilizar SSL 2.0** (*Use SSL 2.0*) caso ainda esteja ativa;



- O **Google Chrome**™ não tem uma função específica para desativar o protocolo SSL v3.0. Assim sendo, é necessário proceder a esta configuração seguindo os seguintes passos: clique no ícone "Google Chrome" com o botão do lado direito do rato e aceda ao menu **Propriedades** (*Properties*) > *tab* **Atalho** (*Shortcut*) > na caixa de texto **Destino** (*Target*) posicione o cursor no final do texto (após o **"**) e digite --ssl-version-min=tls1> confirme esta alteração na opção **OK** e **Continuar** (*Continue*) quando solicitar as permissões de administrador de sistema. De seguida basta reiniciar o computador;

- No **Mozilla Firefox®** sugerimos que consulte a informação disponível no "Mozilla Security Blog";
- Para proceder à desativação SSL v3.0 noutros *browsers* sugerimos que procure por ***Disabling SSLv3 Support in Browsers*** num motor de pesquisa.

Fonte: Millennium bcp

LEMBRE-SE QUE...

Se verificar alguma situação anómala em www.millenniumbcp.pt ou necessitar de esclarecimentos, por favor contacte-nos através do telefone 707 50 24 24 (Atendimento personalizado 24 horas).

Lembre-se que a proteção dos seus dados e computador depende de si!

Fonte: Millennium bcp

SERVIÇO DE ALERTAS
QUER ESTAR SEMPRE INFORMADO?

siga-nos no facebook

Versão portuguesa

HOW CAN YOU PROTECT YOURSELF AGAINST POODLE?

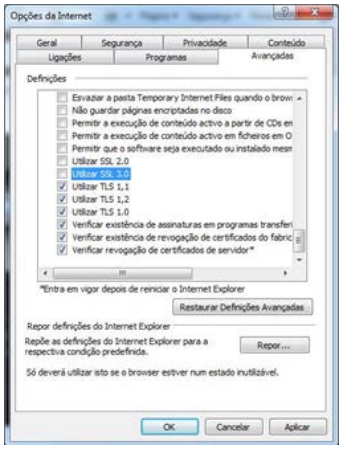
On 14 October, we found that one of the protocols that ensure the safety of communications while accessing bank websites, named protocol SSL v3.0, was vulnerable.

This vulnerability was called POODLE (*Padding Oracle On Downgraded Legacy Encryption*) and enables hackers to obtain encrypted information and even the personal access codes (*passwords*).

The SSL v3.0 (*Secure Sockets Layer, version 3*) is used to establish secure connections between the browsers of the users and the servers of the service providers and diminishes the possibilities of intrusion and capturing data.

However, this protocol is obsolete and the majority of the *browsers* still use it in order to ensure compatibility with older servers. By creating the conditions necessary to explore the vulnerability of the SSL v3.0, the hacker is able to intercept the communications established between the *browser* and the server, force the connection using the SSL v3.0 and, this way, obtain the users information.

This vulnerability affects both users that access bank websites through *browsers* and users that use specific *apps* for that



- **Google Chrome™** does not have a specific function to deactivate the SSL v3.0 protocol. Thus, you have to configure it as follows: click on “Google Chrome” with

purpose.

In spite of the fact that such a security failure is not easy to solve, Millennium bcp was able to promptly respond to the situation and, in less than 24 hours, it was no longer possible to access its servers through the vulnerable protocol.

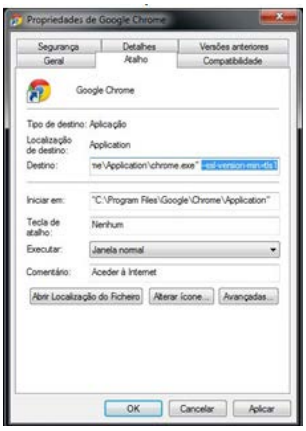
This way, Millennium bcp shows the commitment it has towards the safety experienced by the users of this channel, who continue to be able to safely access their accounts and make their operations in the website of Millennium bcp.

Because safety is one of the priorities of Millennium bcp, it is our duty to, in an active and preventive manner, alert our Customers for situations similar to those described above. You may find all you need to know at millenniumbcp.pt, menu M - Read more: Security and, on the next page, read the "Security Tips".

Below we list some measures that you may adopt to minimize the risk of a hacker attack. These measures vary depending on the *browser* used, for the Windows operating system:

- To deactivate the protocol SSL v3 on the **Internet Explorer® (Windows Vista® or more recent),** go to **Tools** > **Internet Options** > **Advanced** and remove the option **Use SSL 3.0** and **Use SSL 2.0** in case the latter is still active;

the right button of your mouse and go to **Properties** >**Shortcut** >and on the **Target** text box set the cursor at the end of the text (after **"**) and write--ssl-version-min=tls1> confirm this alteration by clicking **OK** and **Continue** when it requests system administrator permissions. Then just restart the computer;



Google and the Google logo are registered trademarks of Google Inc., used with permission.

- When using **Mozilla Firefox®** we suggest that you consult the information provided by the “Mozilla Security Blog”;
- To deactivate the SSL v3.0 on other browsers we suggest you search ***Disabling SSLv3 Support in Browsers*** in a search engine.

Source: Millennium bcp

REMEMBER...

If you ever find something out of place at www.millenniumbcp.pt/en or if you need further information please call us on 707 50 24 24 (Personal Assistance 24/7).

Remember: the protection of your data and computer depends on you!

Source: Millennium bcp

Millennium bcp is resposible for this information