A REVISTA Nº 1 DA TECNOLOGIA

+ INVESTIGAÇÃO
+ REPORTAGEM
+ TUTORIAIS
+ TESTES

DESCOBRIMOS AS MAIORES BURLAS FEITAS AOS OPERADORES

ESPECIAL FORMAÇÃO E EMPREGO
AS MELHORES ESCOLAS E OPORTUNIDADES

EXAME INFORMÁTICA

www.exameinformatica.sapo.pt

COMPARATIVO
QUAL É O MELHOR TABLET DE OITO POLEGADAS?
10 EM CONFRONTO DIRETO
ANDROIT / IOS / WINDOWS

Maio 2014 N.º 227 • Mensal • Ano 18
€3 Portugal Continental • €5,04 Revista + DVD

POUPE + de €500 NA FATURA ENERGÉTICA

TESTADA
GOCYLCLE
ANDÁMOS NA E-BIKE MAIS AVANÇADA DO MUNDO

AS MELHORES PRÁTICAS PARA DIMINUIR NUM ANO AS CONTAS DO GÁS, DA ELETRICIDADE E DO COMBUSTÍVEL

Skoda Yeti Outdoor
Já não é só resistente. Agora também é tecnológico!

INOVAÇÃO
QUADCÓPTERO
O SALVA-VIDAS DAS PRAIAS PORTUGUESAS

TESTES
XPERIA Z2
O TABLET MAIS FINO E LEVE DO MUNDO TAMBÉM TEM DESEMPENHO

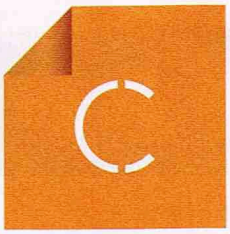
TESTES
ASPIRE S7
O DESIGN IMPRESSIONA, MAS VALE O PREÇO?

TESTES
FOTOGRAFIA
- OLYMPUS OMD M-10
- TOSHIBA CAMILEO X-SPORTS
- SONY CYBER--SHOT DSC-QX100

IMPRESA Publishing
5 603846 017284 00227

HEARTBLEED: DETETADOS 1000 NÚMEROS IP VULNERÁVEIS

Não se sabe que serviços terão sido afetados em Portugal pela maior vulnerabilidade informática dos últimos tempos por Hugo Séneca



Codenomicon e Neel Mehta são nomes desconhecidos da maioria dos entusiastas das tecnologias - mas tiveram direito aos holofotes da ribalta como mensageiros do perigo, ao revelarem, na primeira semana de abril, a existência de uma falha de segurança que terá afetado mais meio milhão de sites e serviços baseados na Internet (estimativa Netcraft). A Codenomicon é uma empresa de segurança eletrónica; Neel Mehta é um investigador da Google: ambos nomes foram apresentados como autores do relatório que dá a conhecer uma falha que afeta versões da encriptação Open SSL, e que pode expor dados confidenciais dos utilizadores de sistemas bancários, contas de e-mail ou redes sociais. Em Portugal, o CERT.pt e a Rede Nacional CSIRT avaliaram o impacto da do Heartbleed em Portugal e detetaram mais de mil números IP vulneráveis.

A estimativa permite descrever o grau de vulnerabilidade em termos numéricos - mas não em termos de importância, recorda Lino Santos, diretor do Centro de Respostas a Incidentes de Segurança (CERT.pt): «A existência de mil números de IP reflete uma taxa de vulnerabilidade reduzida, mas não nos permite saber qual o grau de perigosidade, porque ainda não se sabe quais são os sistemas que têm essa falha e qual a importância esses sistemas nas diferentes áreas de atividade».

DE 1.0.1 A 1.0.1F

O OpenSSL é um sistema de encriptação considerado elementar, que protege comunicações estabelecidas entre internautas e os servidores de um site ou serviço online. A vulnerabilidade Heartbleed explora uma funcionalidade conhecida como "heart beat", que tem o propósito de prolongar as ligações entre internautas e servidores de sites. Os sistemas que usam o Open SSL entre as versões 1.0.1 e 1.0.1f armazenavam nas memórias (dos servidores) passwords e nomes dos utilizadores numa cifra idêntica ao do OpenSSL - e é essa a vulnerabilidade do Heartbleed, que pode ser explorada por quem tem conhecimentos suficientes para aceder aos 64 KB das memórias dos servidores que ficam expostos perante os olhares indiscretos da Web.

A falha detetada no OpenSSL também pode ser encarada como um alerta para o "mundo open source", uma vez que se trata de uma versão em código aberto que é também um componente dos sistemas operativos Linux e de sistemas como o Apache e Nginx que têm grandes quotas no segmento de servidores.

Rui Miguel Silva, líder do laboratório de segurança eletrónica Ubinet, do Instituto Politécnico de Beja, admite que o Heartbleed tenha afetado serviços de a Internet à escala global: «Esta vulnerabilidade pode ser explorada desde 2012, e durante o uso das versões vulneráveis do OpenSSL podem ter sido intercetadas as passwords de muita gente».

O especialista do Ubinet considera ainda que a falha pode afetar de forma generalizada os serviços de Internet, mas aconselha «os gestores de serviços de de alojamento de sites a terem especial atenção para esta falha».

Sérgio Silva, coordenador do departamento de Informática do Conselho Superior de Magistratura, critica a inexistência de iniciativas de sensibilização para este problema: «Facebook, Google e Instagram avisaram os utilizadores e confirmaram vulnerabilidades... como é que em Portugal nenhuma entidade tomou uma posição similar?»

Com a inexistência de uma comunicação para o público, empresas e administração pública evitam assumir o ónus por uma vulnerabilidade de que não são responsáveis, mas também podem estar a atrasar a mudança de passwords e nomes de utilizadores preconizada noutros países: «Os dados dos utilizadores podem ter sido intercetados. Se as pessoas não mudarem as passwords, há a possibilidade de os hackers apenas as usarem dentro de alguns meses, quando já ninguém fala nisto», recorda Sérgio Silva.