CAIS EM RESUMO

MAI14 N.1

Alertas, vulnerabilidades e incidentes de segurança

CAIS EM RESUMO é uma publicação periódica do Centro de Atendimento a Incidentes de Segurança (CAIS/RNP), que tem como objetivo apresentar, de forma reduzida, os principais alertas, vulnerabilidades, tipos de ataque e demais acontecimentos da área de segurança da informação, que impactaram a rede acadêmica e de pesquisa no último quadrimestre.

DESTAQUE

Heartbleed, a falha no OpenSSL

No início de abril desse ano foi descoberta uma vulnerabilidade crítica, presente na biblioteca OpenSSL, conhecida como "*Heartbleed*". Dentre as ações realizadas pelo CAIS, foram publicados dois alertas - um com foco corretivo e outro com foco preventivo.

Foi realizado também um Webinar para toda comunidade acadêmica, com o título "O assunto é Heartbleed", transmitido ao vivo para dezenas de instituições. A gravação deste Webinar pode ser acessada através do Vídeos@RNP, neste link.

Exploração de servidores DNS

O CAIS identificou, no primeiro quadrimestre de 2014, cerca de 15.000 (38% do total) incidentes de tentativa de intrusão explorando uma vulnerabilidade no protocolo DNS. A vulnerabilidade, relacionada a uma configuração errônea do servidor DNS recursivo, permite a realização de ataques de envenenamento de cache (*cache poisoning*). Além disto, pode ser utilizada como fonte de ataques distribuídos de reflexão de negação de serviço (DRDoS).

Ataques a servidores NTP

O CAIS registrou cerca de 300 incidentes de negação de serviço, explorando uma falha no protocolo NTP, no primeiro quadrimestre de 2014. A falha, relacionada a uma configuração incorreta do servidor NTP, permite a execução remota do comando "*monlist*".

Foi publicado o alerta: Ataques de negação de serviço envolvendo o abuso de servidores NTP.

Para saber mais detalhes sobre essa vulnerabilidade, ou saber se seu servidor está vulnerável, bem como as medidas de correção, acesse as referências selecionadas pelo CAIS:

1 - *DNS Amplification Attacks*

2 - Recomendações para Evitar o Abuso de Servidores DNS Recursivos Abertos

Cerca de **15.000**
ataques a servidores DNS

ESTATÍSTICAS

No primeiro quadrimestre de 2014, o CAIS registrou um aumento de 31,5%, em relação ao quadrimestre anterior, na quantidade de incidentes.

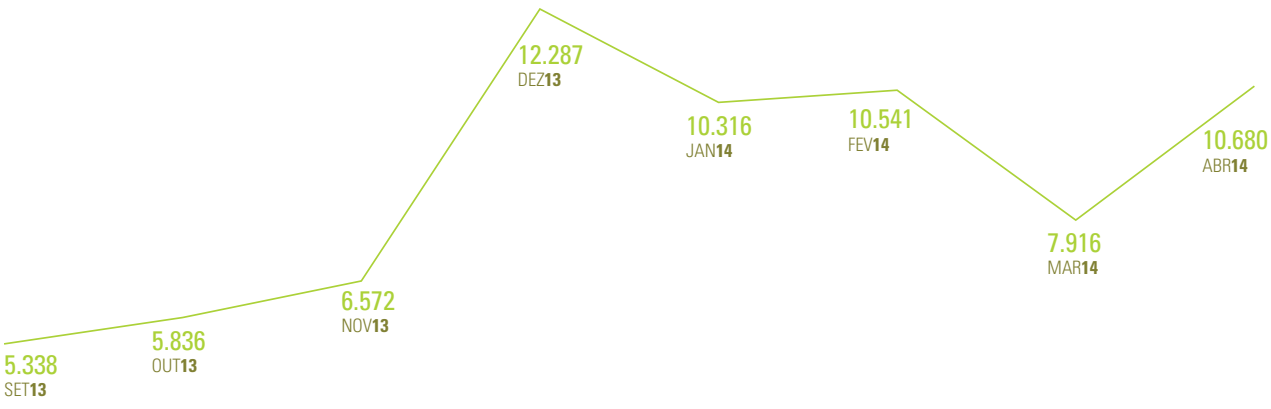
Com exceção das categorias **Conteúdo abusivo**, **Código malicioso** e **Prospecção por informações**, todas as outras tiveram aumento de registro de incidentes.

Impulsionado pela busca por servidores DNS e NTP vulneráveis, a categoria **Tentativa de intrusão** teve um aumento de 140% em relação ao quadrimestre anterior.

Outra categoria que se destacou foi a **Indisponibilidade de serviços**, com um significativo aumento de 180%. Diretamente relacionado à exploração de vulnerabilidades em servidores DNS e NTP, já citado acima na categoria **Tentativa de intrusão**.

TOTAL DE INCIDENTES – QUADRIMESTRES

SET A DEZ 2013	30.033
JAN A ABR 2014	39.453



	2013				2014			
	SET	OUT	NOV	DEZ	JAN	FEV	MAR	ABR
TENTATIVA DE INTRUSÃO	338	263	1.759	6.531	5.539	5.424	4.209	6.226
INDISPONIBILIDADE DE SERVIÇO OU INFORMAÇÃO	8	18	46	38	106	163	7	32

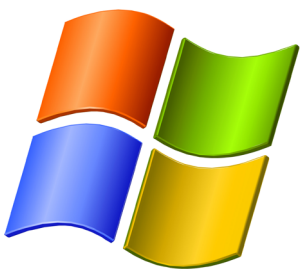
ATUALIZE-SE

Descontinuidade do suporte ao Windows XP

A Microsoft anunciou que no dia 8 de abril de 2014 um dos sistemas operacionais mais utilizados do mundo teria seu suporte descontinuado. O Windows XP, largamente utilizado pela rede acadêmica, apesar de continuar em funcionamento, não receberá novas atualizações. Isto não se limita somente a correção e adição de recursos, como também as atualizações de segurança. Deste modo, o sistema passou a receber ainda mais atenção de ameaças virtuais.

Vulnerabilidades descobertas a partir dessa data poderão ser exploradas em larga escala, haja visto que não haverá correção por parte do fabricante.

A principal recomendação do CAIS é atualizar o sistema operacional para uma versão mais recente. Saiba mais no alerta publicado.



REFERÊNCIAS

Segue uma lista de documentos utilizados como referência nesta publicação. Recomendamos a sua leitura como modo de complementar os conceitos aqui tratados.

CAIS-Alerta: Vulnerabilidade no OpenSSL
http://www.rnp.br/cais/alertas/2014/openssl.html

CAIS-Alerta: Vulnerabilidade no OpenSSL - Atualização 1
http://www.rnp.br/cais/alertas/2014/openssl_1.html

Webinar - O assunto é Heartbleed
http://video.rnp.br/portal/video.action?idItem=21724

CAIS-Alerta: Ataques de negação de serviço envolvendo o abuso de servidores NTP
https://www.rnp.br/cais/alertas/2014/NTP.html

DNS Amplification Attacks
https://www.us-cert.gov/ncas/alerts/TA13-088A

Recomendações para evitar o abuso de servidores DNS recursivos abertos
http://www.cert.br/docs/whitepapers/dns-recursivo-aberto

CAIS-Alerta: Suporte ao sistema operacional Windows XP descontinuado
http://www.rnp.br/cais/alertas/2014/suporte-windows-xp.html

RNP
Rede Nacional de Ensino e Pesquisa

Nelson Simões
Diretor Geral

José Luiz Ribeiro Filho
Diretor de Serviços e Soluções

Realização:

CAIS
Centro de Atendimento a Incidentes de Segurança da RNP

Liliana Velásquez Solha
Gerente de Segurança da Informação

Redação:
Alan Santos, Ana Carolina Fukushima, Edilson Lima e Rildo Souza

Contribuições:
André Landim, Carla Freitas, Cristiane Rodrigues, Júlio Henrique, Ronald Huppers, Thais Godinho, Vanessa Suzuki e Yuri Alexandro

Projeto visual e Diagramação:
Tecnodesign