CAIS EM RESUMO JAN15 N.3

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 resumida, 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

Shellshock

O Shellshock, considerado tão crítico quanto o Heartbleed, é uma vulnerabilidade que atinge o interpretador de comandos *Bash*, o mais popular em sistemas Unix.

A sua exploração pode permitir o acesso de pessoas não autorizadas a um servidor vulnerável, ganhando-se consequentemente acesso a dados e a informações críticas, como usuários, senhas e arquivos confidenciais.

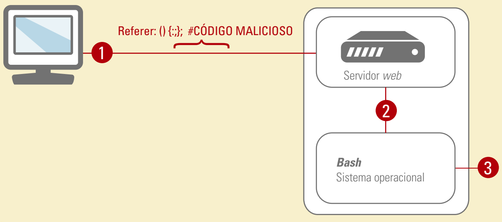
Embora o Shellshock possa afetar qualquer servidor que execute *Bash* em uma versão vulnerável, a vulnerabilidade só pode ser explorada por um atacante remoto em circunstâncias específicas. Para um ataque ser bem-sucedido, o atacante precisará forçar uma aplicação a enviar ao *Bash* uma variável de ambiente com conteúdo malicioso.

Nesse sentido, o vetor de ataque mais utilizado tem sido o CGI (Common Gateway Interface), método amplamente usado por servidores *web* para geração de conteúdo *web* dinâmico. Um atacante pode, via CGI, enviar um comando malicioso, definindo uma variável de ambiente mal formada. Como o servidor usa *Bash* como interpretador, o comando malicioso será executado.

Os principais sistemas afetados são baseados em Unix, como Linux e Mac OS X.

Mesmo assim, outros sistemas podem ser afetados. Isso porque o *Bash* pode executar comandos enviados por *scripts* CGI, que é uma forma usada por páginas *web* para gerar conteúdo dinâmico, com base nas entradas do usuário, o que aumenta consideravelmente o número de usuários impactados.

A exploração ocorre da seguinte forma:



1. O atacante envia código malicioso para o servidor *web*.
2. O servidor *web* envia a instrução ao *bash*, que a executa.
3. O atacante pode, então, executar diversas ações:
   - Roubar arquivos de senhas;
   - Fazer *downloads* via WGET;
   - Criar sessões para acesso direto ao sistema, entre outros.

Saiba mais sobre a vulnerabilidade no alerta enviado pelo CAIS.

Poodle, a vulnerabilidade no SSLv3

A vulnerabilidade, divulgada em outubro de 2014, evidenciava uma falha na implementação do protocolo SSLv3.

Utilizado massivamente para cifrar conexões em sites e serviços de e-mail na internet, pode permitir que um atacante utilize a técnica de *man-in-the-middle* para interceptar e decifrar conexões seguras como o acesso a contas bancárias, compras e pagamentos via internet, por exemplo.

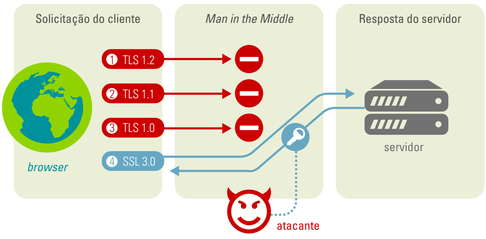
No final de 2014 foram encontradas vulnerabilidades em algumas implementações específicas do protocolo TLS presentes em equipamentos Cisco, BlueCoat, F5 Networks, A10 Networks entre outros. No entanto, o protocolo TLS sem alterações não é vulnerável ao ataque.

Na rede Ipê, mais de 4 mil *hosts* vulneráveis foram detectados desde o começo do mês de novembro.

O CAIS recomenda que seja desabilitado o uso do protocolo SSLv3 tanto no cliente como no servidor. Quando for necessário suportar esse protocolo, a recomendação é utilizar SCSV (*Signaling Cipher Suite Value*).

As versões do protocolo TLS 1.0, 1.1 e 1.2 não são vulneráveis. Somente a versão do SSL 3.0 permanece vulnerável.

Saiba mais sobre a vulnerabilidade Poodle em Referências.



ESTATÍSTICAS

No terceiro quadrimestre de 2014, o CAIS registrou quase 200 mil notificações, o que totaliza mais de 420 mil notificações no ano de 2014.

As principais notificações do terceiro quadrimestre foram:

Hosts vulneráveis que podem ser utilizados para ataques de negação de serviço

Aumento de 7%, aproximadamente, nas notificações de *hosts* com serviços (NetBios, SSDP e SNMP) configurados de forma a permitir consultas externas não autorizadas.

A exploração dessa vulnerabilidade permite ao atacante realizar um ataque de negação de serviço e, consequentemente, indisponibilizar o *host* ou a rede relacionada ao sistema atacado.

Incidentes de desfiguração de sites

No terceiro quadrimestre foi registrado um aumento de mais de 100% no número de desfiguração em páginas de clientes da RNP. Os atacantes exploraram principalmente vulnerabilidades no servidor *web* Apache, MySQL e aplicações PHP.

Os servidores atacados foram utilizados, em sua maioria, como repositórios de *malware* e sites de *phishing*, como constatou o CAIS.

Mais de 420 mil
notificações em 2014

TOTAL DE NOTIFICAÇÕES NO 3º QUADRIMESTRE 2014 – 196.165

ATUALIZE-SE

No dia 1º de dezembro de 2014, foi lançado pela RNP o Sistema de Gerenciamento de Incidentes de Segurança (SGIS). Com o novo sistema, todas as organizações usuárias poderão gerenciar seus incidentes de segurança de maneira mais simples e eficaz. A ferramenta oferece vários recursos aos administradores:

* Gerenciamento e acompanhamento dos incidentes de segurança através de indicadores e relatórios gerenciais *online*
* Acesso a dados de incidentes e vulnerabilidades de forma segregada
* Possibilidade de recebimento de notificações de incidentes em formato XML
* Acesso a base de conhecimento através de ferramenta colaborativa (wiki)

Além dos recursos citados acima, com o intuito de garantir a confidencialidade, integridade e autenticidade dos dados abrigados, um rigoroso processo de autenticação e autorização de acesso ao sistema foi estabelecido, baseado em segregação de perfis que, por sua vez, respeita a cadeia de confiança entre os diversos usuários do sistema. O serviço de tratamento a incidentes de segurança é oferecido pela RNP a todas as organizações usuárias da rede Ipê, sendo o SGIS um instrumento crucial de apoio neste sentido.

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 *Bash* permite execução remota de código
http://www.rnp.br/sites/default/files/cais-alerta-bash-1.pdf

CAIS-Alerta: início do horário de verão 2014/2015
http://www.rnp.br/sites/default/files/alerta-cais-horario-verao-2014-1.pdf

CAIS-Alerta: Vulnerabilidades no BIND
http://www.rnp.br/sites/default/files/cais-alerta-bind.pdf

The Poodlebleed Bug
http://poodlebleed.com/

This POODLE Bites: Exploiting The SSL 3.0 Fallback
https://www.openssl.org/~bodo/ssl-poodle.pdf

SSL 3.0 Protocol Vulnerability and POODLE Attack
https://www.us-cert.gov/ncas/alerts/TA14-290A

POODLE Vulnerability Puts Online Transactions At Risk
http://blog.trendmicro.com/trendlabs-security-intelligence/poodle-vulnerability-puts-online-transactions-at-risk/

Bash Code Injection Vulnerability via Specially Crafted Environment Variables (CVE-2014-6271, CVE-2014-7169)
https://access.redhat.com/articles/1200223
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-6271
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-7169

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, Edilson Lima e Rildo Souza

Revisão:
Ana Carolina Fukushima, Carla Freitas, Vanessa Suzuki e Yuri Alexandro

Projeto visual e Diagramação:
Tecnodesign