Presidência da República
Gabinete de Segurança Institucional
Departamento de Segurança da Informação e Comunicações
Centro de Tratamento de Incidentes de Segurança de Redes de Computadores da Administração Pública Federal

Alerta nº 07/2014 – Shellshock/Bash – CVE 2014-6271 e CVE 2014-7169

Revisão nº 01 - Exploração dos Servidores Apache HTTP, OpenSSH e DHCP

1. Descrição do Problema

O interpretador de comandos Bourne-Again Shell, ou simplesmente Bash, utilizado por sistemas Linux, Unix e Mac OS, permite a execução arbitrária de comandos de forma remota.

O relatório CVE-2014-6271, do NIST, definiu o nível de severidade dessa vulnerabilidade com o valor 10, o mais alto em sua classificação. Devido a ampla utilização do Bash em diversos sistemas computacionais, as possibilidades de exploração são inúmeras, justificando seu alto grau de impacto às atividades da organização.

Após novas investigações, foi publicado por meio do relatório CVE-2014-7169, também do NIST, novo "bug" relacionado ao Bash. Segundo a publicação, a falha permite explorar servidores OpenSSH, utilizando uma funcionalidade denominada "ForceCommand", servidores Apache HTTP, que utilizam Common Gateway Interface (CGI), por meio dos módulos "mod_cgi" e "mod_cgid", e servidores DHCP, por meio da execução de scripts no momento da requisição de IP.

O NIST informa que esta vulnerabilidade existe devido a uma correção incompleta para CVE-2014-6271.

Ainda, segundo o NIST, é possível realizar ataques de forma simples, por meio da rede, sem necessariamente passar pelo mecanismo de autenticação, manipulando variáveis de ambiente. Utilizando-se de uma facilidade que permite a injeção de código no conteúdo, um script malicioso pode ser implementado em qualquer variável de ambiente, permitindo ao invasor a execução de qualquer comando.

Para certificar-se da existência da vulnerabilidade, a Red Hat sugere a execução do seguinte comando:

```
$ env x='() { :;}; echo vulnerable' bash -c "echo this is a test"
```

Caso confirmada a vulnerabilidade, a seguinte saída será exibida:

```
vulnerable… this is a test
```

Caso negativo, poderá ser exibida a seguinte saída:

```
bash: warning: x: ignoring function definition attempt
bash: error importing function definition for `x'
this is a test
```

De acordo com o sistema de divulgação de vulnerabilidades do National Institute of Standards and Technology (NIST), National Vulnerability Database (NVD), todas as versões desde 1994 (1.14.0) até a versão 4.3 (fevereiro/2014) apresentam a falha.

2. Possíveis Riscos

Acesso a informações da organização sem necessidade de permissionamento adequado;

Modificação não autorizada de qualquer ativo de informação;

Comprometimento de quaisquer serviços;

3. Ameaças

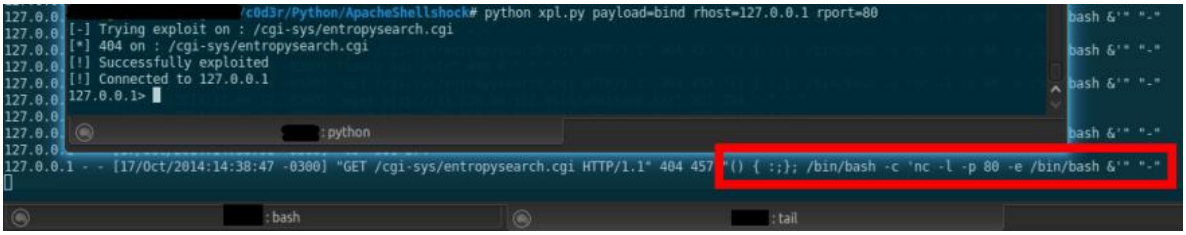
a. Por meio de monitoramento de canais IRC, realizado por um CSIRT integrante da comunidade internacional, tomamos conhecimento da infecção de diversos sistemas, incluindo domínios do governo brasileiro, por um malware conhecido por "LinuxNet perlbot", utilizado pelos atacantes para exploração dessa vulnerabilidade. Estes sistemas estavam sendo controlados por meio de um servidor IRC, conforme extrato de log a seguir:

---

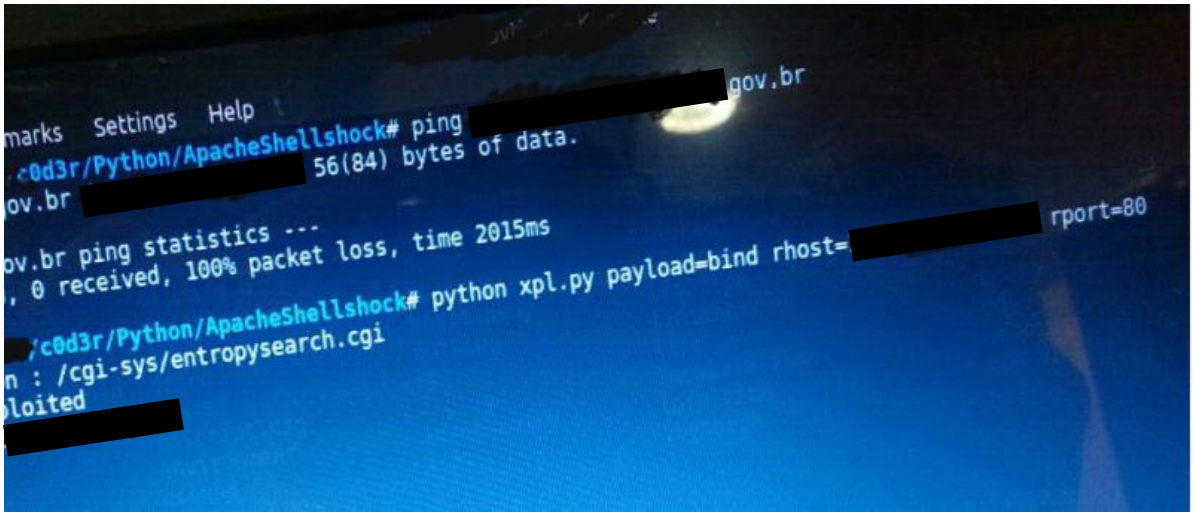
irc_user host
|PHP|210159 PHP xpower-3100BB83.xxx.jus.br Linux 2.6.32-29-server
xxx.jus.br
|PHP|438034 PHP xpower-34779A77.xxx.xx.gov.br Linux
2.6.26-2-686-bigmem xxxx.xx.gov.br

---

b. Outra ameaça, divulgada pelo Centro de Defesa Cibernética, do Ministério da Defesa, e identificada por meio de acompanhamento de fontes abertas, refere-se a um exploit escrito na linguagem Python, voltado para explorar servidores Apache ("ApacheShellshock"):

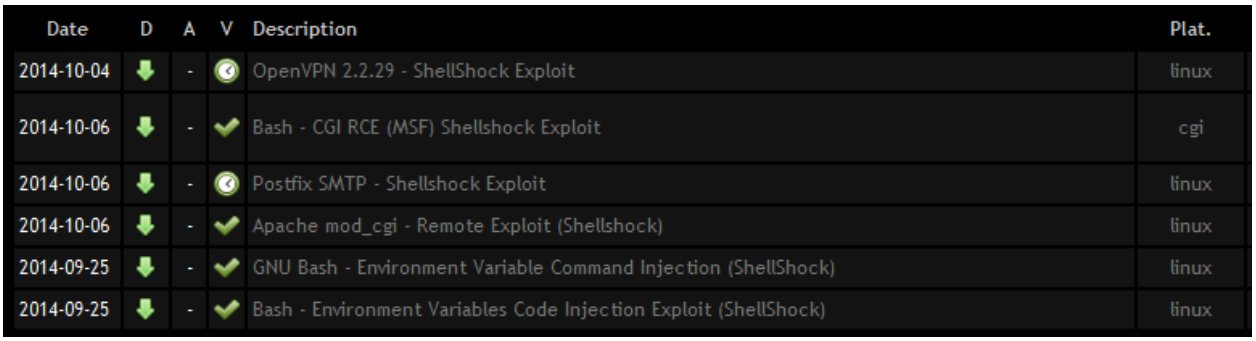


Fonte: http://unknownsec.wordpress.com/?ref=spelling



Fonte: http://unknownsec.wordpress.com/?ref=spelling

c. O serviço Exploit Database (http://www.exploit-db.com) possui uma lista de ferramentas desenvolvidas para exploração dessa vulnerabilidade:



Date	D	A	V	Description	Plat.
2014-10-04		-		OpenVPN 2.2.29 - ShellShock Exploit	linux
2014-10-06		-		Bash - CGI RCE (MSF) Shellshock Exploit	cgi
2014-10-06		-		Postfix SMTP - Shellshock Exploit	linux
2014-10-06		-		Apache mod_cgi - Remote Exploit (Shellshock)	linux
2014-09-25		-		GNU Bash - Environment Variable Command Injection (ShellShock)	linux
2014-09-25		-		Bash - Environment Variables Code Injection Exploit (ShellShock)	linux

4. Sugestões para Mitigação do Problema

O desenvolvedor do interpretador de comandos “Bash” disponibilizou um patch de correção, que pode ser encontrado no seguinte repositório:

- http://ftp.unicamp.br/pub/gnu/bash/bash-4.3-patches/

Baseado na correção desenvolvida, diversas distribuições Linux, como CentOS, Debian, Ubuntu e Red Hat, já disponibilizaram em seus repositórios uma correção para a falha. Para a distribuição Debian, o serviço Debian Security Advisory disponibilizou a seguinte atualização de segurança:

- https://www.debian.org/security/2014/dsa-3032

Referências:

- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271
- http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-7169
- http://ftp.unicamp.br/pub/gnu/bash/
- http://searchsecurity.techtarget.com/news/2240231414/In-Heartbleeds-wake-Bash-shell-flaw-puts-Linux-Mac-OS-users-at-risk
- https://www.us-cert.gov/ncas/current-activity/2014/09/24/Bourne-Again-Shell-Bash-Remote-Code-Execution-Vulnerability
- https://www.debian.org/security/
- https://access.redhat.com/node/1207723
- http://lists.centos.org/pipermail/centos/2014-September/146099.html
- http://www.ubuntu.com/usn/usn-2362-1/
- https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/
- http://lcamtuf.blogspot.com.br/2014/09/quick-notes-about-bash-bug-its-impact.html

Brasília-DF, 20 de Outubro de 2014

Atenciosamente,

Equipe do CTIR Gov