Alerta de Segurança 006/2014 - CGTI/VPGDI

Em 26 de setembro de 2014

Para: Gestores de TI das unidades da Fiocruz
Assunto: Shellshock/Bash

Prezados Gestores,

Encaminhamos, na íntegra, o alerta emitido pela Coordenação-Geral de Tratamento e Incidentes de Redes / Departamento de Segurança da Informação e Comunicações sobre o interpretador de comandos Bourne-Again Shell (Bash).

## 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.

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. 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://ftp.unicamp.br/pub/gnu/bash/
- http://searchsecurity.techtarget.com/news/2240231414/In-Heartbleeds-wake-Bash-shell-flawputs-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-variablescode-injection-attack/
- http://lcamtuf.blogspot.com.br/2014/09/quick-notes-about-bash-bug-its-impact.html


Atenciosamente,

Coordenação de Gestão de Tecnologia da Informação
Segurança da Informação e Comunicações