CAIS-Alerta: Vulnerabilidade no Bash permite execução remota de código

[RNP, 25.09.2014]

O CAIS alerta sobre uma recente vulnerabilidade de exploração remota presente no Bash, nas versões 4.3 e anteriores. O Bash é o interpretador de comandos padrão da maioria das distribuições Linux e outros sistemas *BSD e UNIX Like.

Impacto

A falha está relacionada à forma como o Bash processa variáveis de ambiente passadas ao sistema operacional, por programas que solicitam um script bash-based.

Um usuário mal intencionado poderia executar remotamente comandos arbitrários contra uma aplicação web que execute scripts CGI, por exemplo, ou contra sessões SSH em casos específicos.

Versões afetadas

Todas as versões anteriores do GNU BASH, inclusive, a 4.3.

Verificações

Para verificar se o seu ambiente está vulnerável, execute:

env x='() { :;}; echo vulneravel' bash -c "echo isto e um teste"

Se a saída for:

vulnerável

isto é um teste

O sistema está vulnerável.

Caso a saída seja:

bash: warning: x: ignoring function definition attempt

bash: error importing function definition for `x'

isto é um teste

O sistema não está vulnerável.

Mais informações

https://access.redhat.com/articles/1200223

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2014-6271

http://www.csoonline.com/article/2687265/application-security/remote-exploit-in-bash-cve-2014-6271.html

https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/

http://arstechnica.com/security/2014/09/bug-in-bash-shell-creates-big-security-hole-on-anything-with-nix-in-it/

Identificadores CVE (http://cve.mitre.org)

CVE-2014-6271, CVE-2014-7169

O CAIS recomenda que os administradores mantenham seus sistemas e aplicativos sempre atualizados, de acordo com as últimas versões e correções oferecidas pelos fabricantes.

Os alertas do CAIS também são oferecidos no formato RSS/RDF e no

Twitter:

http://www.rnp.br/cais/alertas/rss.xml

Siga @caisrnp