CAIS-Alerta: Vulnerabilidade envolvendo a GNU C Library (glibc)

[RNP, 28.01.2015]

O CAIS alerta para uma vulnerabilidade envolvendo a GNU C Library (glibc), um componente amplamente utilizado nas distribuições Linux, que pode permitir a atacantes executarem código arbitrário em sistemas e obter o controle do sistema operacional.

Até o momento da publicação desse alerta, não foram divulgados códigos de exploração para a vulnerabilidade listada.

Descrição

Um usuário mal intencionado pode obter controle total do sistema afetado, de forma remota.

Sistemas impactados

A glibc é um componente importante para grande parte dos serviços disponíveis em sistemas Linux; por exemplo, serviços que façam resolução de nomes utilizando uma das chamadas gethostbyname() ou gethostbyname2(), estão vulneráveis.

Versões afetadas

Da versão 2.2 até a versão 2.17. As distribuições do Linux que utilizam glibc-2.18 em diante, não são afetadas.

Correções disponíveis

Atualizar a versão da GNU C Library (glibc) para a versão mais recente disponível para o sistema operacional. É recomendada a reinicialização do servidor após a atualização, devido a quantidade de serviços que utilizam a biblioteca afetada.

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

CVE-2015-0235

Mais informações

https://www.qualys.com/research/security-advisories/GHOST-CVE-2015-0235.txt

https://security-tracker.debian.org/tracker/CVE-2015-0235

https://access.redhat.com/security/cve/CVE-2015-0235

http://www.ubuntu.com/usn/usn-2485-1/

http://lists.centos.org/pipermail/centos-announce/2015-January/020906.html

https://community.qualys.com/blogs/laws-of-vulnerabilities/2015/01/27/the-ghost-vulnerability

https://www.us-cert.gov/ncas/current-activity/2015/01/27/Linux-Ghost-Remote-Code-Execution-Vulnerability

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 **Twitter:**

Siga @caisrnp