Prezados,

O CAIS alerta para a recente vulnerabilidade encontrada em sistemas operacionais Linux, FreeBSD, NetBSD, OpenBSD e Solaris, versões de 32 e 64 bits, que permite a um usuário malicioso executar códigos arbitrários e obter elevação de privilégios dentro do sistema. Já foram desenvolvidos códigos de exploração para a vulnerabilidade identificada.

Descrição

A vulnerabilidade está na forma em que os sistemas operacionais afetados gerenciam a memória. O sistema, na execução de uma aplicação, aloca, por padrão, determinado espaço de memória conhecida como stack (pilha), a qual pode crescer automaticamente quando a aplicação necessitar de mais memória. Contudo, se o programa requisita a alocação de muita memória e a stack cresce demasiadamente, ela pode "colidir" com o espaço alocado para outra stack e fazer com que o programa confunda as regiões de memória e execute códigos arbitrariamente. Um usuário malicioso pode explorar essa condição para chocar propositalmente o espaço de uma stack com outra, utilizando os espaços de memória reservados para outra stack e assim executar códigos para obter acesso de root completo.

A vulnerabilidade afeta todas as distribuições do Linux, FreeBSD, OpenBSD, NetBSD e Solaris, tanto nas versões i386 (32 bits) e amd64 (64 bits). Até o momento, há registros da exploração em ambiente local utilizando o programa ld.so e os aplicativos EXIM, SUDO, AT e RSH, além de provas de conceito em implementações de funções específicas de gerenciamento de stack. Apesar de não haver registros até o momento, a possibilidade de exploração remota desta vulnerabilidade não está descartada.

Sistemas impactados

Sistemas operacionais Linux (Debian, Red Hat, Suse, entre outros)
Sistemas operacionais FreeBSD
Sistemas operacionais NetBSD
Sistemas operacionais OpenBSD
Sistemas operacionais Solaris

Versões afetadas

Todas as distribuições nas versões i386 e adm64.

Correções disponíveis

Atualizar os sistemas operacionais afetados para as versões mais recentes fornecidos pelos desenvolvedores.

Identificadores CVE (http://cvw.mitre.org)
CVE-2010-2240

CVE-2016-3672
CVE-2017-1083
CVE-2017-1084
CVE-2017-1085
CVE-2017-3629
CVE-2017-3630
CVE-2017-3631
CVE-2017-1000365
CVE-2017-1000366
CVE-2017-1000367
CVE-2017-1000369
CVE-2017-1000370
CVE-2017-1000371
CVE-2017-1000372
CVE-2017-1000373
CVE-2017-1000374
CVE-2017-1000375
CVE-2017-1000376
CVE-2017-1000377
CVE-2017-1000379

Mais informações

https://www.qualys.com/2017/06/19/stack-clash/stack-clash.txt
https://blog.qualys.com/securitylabs/2017/06/19/the-stack-clash
https://lists.debian.org/debian-security-announce/2017/msg00146.html
https://lists.debian.org/debian-security-announce/2017/msg00148.html
https://lists.debian.org/debian-security-announce/2017/msg00147.html
https://lists.debian.org/debian-security-announce/2017/msg00149.html

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 podem ser acompanahadas pelas redes sociais da RNP. Siga-nos!
Twitter: @RedeRNP
Facebook: facebook.com/RedeNacionaldeEnsinoePesquisaRNP.

```
#####################################################################
#   CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)     #
#       Rede Nacional de Ensino e Pesquisa (RNP)               #
#                                                              #
# cais@cais.rnp.br       http://www.rnp.br/servicos/seguranca  #
# Tel. 019-37873300      Fax. 019-37873301                     #
# Chave PGP disponivel   http://www.rnp.br/cais/cais-pgp.key   #
#####################################################################
```