CAIS-Alerta: Vulnerabilidades envolvendo servidores de arquivos Samba (smbd)

[RNP, 24.02.2015]

O CAIS alerta para uma vulnerabilidade recente envolvendo o servidor de arquivos Samba. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para a vulnerabilidade listada.

Descrição

Um cliente malicioso pode enviar pacotes *netlogon* manipulados que, quando processados pelo *daemon smbd*, podem potencialmente executar códigos arbitrários no sistema, com as mesmas permissões do usuário executando o *daemon* (por padrão, o usuário root). Não sendo necessária nenhuma autenticação para explorar esta vulnerabilidade.

Sistemas impactados

Sistemas utilizando o Samba entre as versões 3.5.0 e 4.2.0rc4

Versões afetadas

Versões anteriores a 4.2.0rc5, 4.1.17, 4.0.25 e 3.6.25

Correções disponíveis

Atualizar a versão do Samba para a versão mais recente disponível pelos desenvolvedores (4.2.0rc5, 4.1.17, 4.0.25 e 3.6.25, no momento da publicação deste alerta) ou a versão mais recente recomendada de acordo com o sistema operacional em uso. É recomendada a reinicialização do serviço após a atualização.

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

CVE-2015-0240

Mais informações

https://www.samba.org/samba/security/CVE-2015-0240

http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2015-0240

https://access.redhat.com/articles/1346913

http://www.ubuntu.com/usn/usn-2508-1

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