CAIS-Alerta: Vulnerabilidades envolvendo servidores NTP (NTPd)

[RNP, 06.02.2015]

O CAIS alerta para duas vulnerabilidades recentes envolvendo o serviço NTP (ntpd). Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para a vulnerabilidade listada.

Descrição

Um usuário pode, através da manipulação de valores que não são corretamente validados em alguns trechos de código, causar negação de serviço ou vazamento de informações; além disso, também é possível burlar ACLs que utilizem o endereço IPv6 ::1 (localhost) em alguns sistemas operacionais.

Sistemas impactados

Sistemas operacionais que utilizem a implementação NTP do projeto ntp.org

Versões afetadas

Todas as versões anteriores a 4.2.8p1 (de acordo com o projeto NTP.Org)

Correções disponíveis

Atualizar a versão do NTP para a versão mais recente disponível pelos desenvolvedores (4.2.8p1, 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-2014-9297 CVE-2014-9298

Mais informações

http://support.ntp.org/bin/view/Main/SecurityNotice#Recent_Vulnerabilities

https://www.kb.cert.org/vuls/id/852879

https://security-tracker.debian.org/tracker/DSA-3154-1

https://access.redhat.com/security/cve/CVE-2014-9297

https://access.redhat.com/security/cve/CVE-2014-9298

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