CAIS-Alerta: Vulnerabilidade no Bind 9

[RNP, 03.11.2016]

O CAIS alerta para uma vulnerabilidade recente envolvendo o servidor de nomes (DNS) Bind9. Até o momento da publicação deste alerta, não foram divulgados códigos de exploração para a vulnerabilidade listada; porém, a consulta que pode desencadear o problema já foi debatida em listas de discussão públicas.

Descrição

Um defeito no tratamento do Bind nas respostas recursivas que contenham um registro DNAME, pode causar o término do daemon após encontrar uma falha, causando indisponibilidade (negação de serviço / DoS) para os clientes. Um atacante remoto pode explorar esta vulnerabilidade sem nenhuma autenticação.

Sistemas impactados

Sistemas utilizando o Bind9 em versões 9.9.x anteriores a 9.9.9-P4, versões 9.10.x anteriores a 9.10.4-P4, e versões 9.11.x anteriores a 9.11.0-P1

Versões afetadas

Versões anteriores a 9.9.9-P4, 9.10.4-P4 e 9.11.0-P1

Correções disponíveis

Atualizar a versão do Bind para a versão mais recente disponibilizada pelos desenvolvedores (9.9.9-P4, 9.10.4-P4 e 9.11.0-P1 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-2016-8864

Mais informações
https://kb.isc.org/article/AA-01434
http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2016-8864
https://www.debian.org/security/2016/dsa-3703
https://www.ubuntu.com/usn/usn-3119-1/
https://access.redhat.com/security/cve/cve-2016-8864
https://www.suse.com/security/cve/CVE-2016-8864.html
http://www.securityfocus.com/bid/94067

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

Atenciosamente,
CAIS/RNP