Giovani

De: Anderson Lima [vlfanderson@ceasaminas.com.br]
Enviado em: quinta-feira, 21 de fevereiro de 2019 13:50
Para: giovani@ceasaminas.com.br
Assunto: Fw: [ALERTA DE SEGURANÇA DA INFORMAÇÃO] DNS recursivo aberto - CEASA MINAS|200.198.51.252 - 1ª Notificação

PSC

Anderson Aparecido de Lima | Detin
Gestor do Departamento de Tecnologia da Informação
Telefone: +55 31 3399-2084
Celular : +55 31 98222-3208
www.ceasaminas.com.br

-----Mensagem Original-----
From: CERT.br
Sent: Thursday, February 21, 2019 1:44 PM
To: Anderson Lima
Cc: cert@cert.br
Subject: Re: [ALERTA DE SEGURANÇA DA INFORMAÇÃO] DNS recursivo aberto - CEASA MINAS|200.198.51.252 - 1ª Notificação

Caro Anderson,

Agradecemos a rápida resposta e as medidas tomadas.

Atenciosamente,
--
Luiz Eduardo Roncato Cordeiro
CERT.br/NIC.br
<cert@cert.br>
https://www.cert.br/

----- Original message -----
From: Anderson Lima <vlfanderson@ceasaminas.com.br>
To: ctis@prodemge.gov.br, "Gerencia de Atendimento, GAT"
<atendimento@prodemge.gov.br>
Cc: "CERT, Cert" <cert@cert.br>, CTIS Centro de Tratamento de Incidentes de Seguranca <ctis@prodemge.gov.br>, Leomar de Araujo Moreira <leomar@prodemge.gov.br>, "MG, Registro" <registro@mg.gov.br>
Subject: Re: [ALERTA DE SEGURANÇA DA INFORMAÇÃO] DNS recursivo aberto -
CEASA MINAS|200.198.51.252 - 1ª Notificação
Date: Thu, 21 Feb 2019 13:38:03 -0300
Message-ID: <49C662E20D7441B28254F2E5F9CA154B@ceasaminas.local>
In-Reply-To: <7da7-5c6ebf80-15-4ce7f200@182004053>
References: <7da7-5c6ebf80-15-4ce7f200@182004053>
X-Mailer: Microsoft Windows Live Mail 16.4.3528.331

Boa tarde, Prezados!

Foi desativado o serviço de NetBios sobre IP, é possível verificar se a medida solucionou o problema?

No aguardo,

Anderson Aparecido de Lima | Detin

Gestor do Departamento de Tecnologia da Informação
Telefone: +55 31 3399-2084
Celular : +55 31 98222-3208
www.ceasaminas.com.br

From: ctis@prodemge.gov.br
Sent: Thursday, February 21, 2019 12:10 PM
To: vlfanderson@ceasaminas.com.br ; Gerencia de Atendimento, GAT
Cc: CERT, Cert ; CTIS Centro de Tratamento de Incidentes de Seguranca ; Leomar de Araujo Moreira ; MG, Registro
Subject: [ALERTA DE SEGURANÇA DA INFORMAÇÃO] DNS recursivo aberto - CEASA MINAS|200.198.51.252 - 1ª Notificação

À Centrais de Abastecimento de Minas Gerais - CEASAMINAS.

Foi identificado que os servidores de endereço IP 200.198.51.252, pertencente a CEASA MINAS, está com o serviço de DNS Recursivo Aberto tornando-se vulneráveis à ataques de negação de serviços.

Para minimizar o risco de que incidentes de segurança da informação ocorram neste servidor, solicitamos a correção imediata desta vulnerabilidade e das demais que possam existir.

Recomendamos que seja realizado um scan de vulnerabilidades.

Qualquer dúvida, estamos a disposição.
Atenciosamente,

CTIS – Centro de Tratamento de Incidentes de Segurança
Tel: +55 31 3339-1215
INOC-DBA: 10670*800
PRODEMGE - Companhia de Tecnologia da Informação do Estado de Minas Gerais
Aviso: Esta mensagem é destinada exclusivamente para a(s) pessoa(s) a quem é dirigida, podendo conter informação sigilosa e legalmente protegida. O uso impróprio será tratado conforme as normas da empresa e a legislação em vigor. Caso não seja o destinatário, favor notificar o remetente, ficando proibidas a utilização, divulgação, cópia e distribuição

-------- Original Message --------
Assunto: Alerta: [AS 10670] servico NetBIOS habilitado
Data: Quinta, Fevereiro 21, 2019 10:06 -03
De: "CERT.br" <cert@cert.br>
Responder-Para: cert@cert.br
Organização: Computer Emergency Response Team Brazil
Para: abuse@prodemge.gov.br, ctir@ctir.gov.br
CC: cert@cert.br

Caro responsavel,

Os IPs presentes no log abaixo sao de servidores sob sua responsabilidade com o servico NetBIOS (137/udp) habilitado. Este servico pode ser abusado para fazer parte de ataques distribuidos de negacao de servico, consumindo recursos da sua rede e impactando terceiros, alem de poder revelar informacoes sensiveis armazenadas neste equipamento.

Gostariamos de solicitar que:

* o servico NetBIOS seja acessivel apenas `a sua rede local, ou que
desabilite o servico no equipamento, caso ele nao esteja em uso.

Uma descricao do problema e possiveis solucoes podem ser encontradas no
final deste documento.

Se voce nao for a pessoa correta para corrigir o problema destes
servidores com o servico NetBIOS habilitado, por favor repasse essa
mensagem para alguem de sua organizacao que possa faze-lo.

O indicador no campo 'Resultados do Teste' indica o tipo de problema
testado e significa:

* netbios: status/pacotes/bytes, onde status e' "open", e
pacotes/bytes indicam o tamanho da resposta recebida, em
pacotes/bytes;

==========
Endereco IP | ASN | Status | Data do Teste | Resultados do Teste
200.198.51.252 | 10670 | OPEN | 2019-02-21T12:53:56Z | netbios: open/1/175
==========

Mais detalhes sobre o porque do envio desta mensagem, quem e' o
CERT.br e como resolver este problema estao listados abaixo.

Cordialmente,
--
CERT.br
<cert@cert.br>
https://www.cert.br/

* O que e' o servico NetBIOS (137/udp)?

O servico NetBIOS e' utilizado tipicamente por sistemas Microsoft
Windows, ou sistemas Unix atraves do Samba, para compartilhamento de
arquivos e impressoras.

Por se tratar de um servico geralmente utilizado apenas dentro de
redes locais e com sistemas anteriores ao Microsoft Windows 2000, e'
muito provavel que nao exista necessidade do servico NetBIOS estar
exposto `a Internet.

Caso esteja acessivel a toda a Internet via UDP, esse servico pode
ser explorado para ataques DDoS que usem amplificacao. Isto ocorre
porque o atacante envia uma requisicao forjando o IP da vitima e o
servidor com NetBIOS retorna uma resposta muito maior que a
requisicao.

* Por que devo me preocupar com isso?

O NetBIOS pode ser abusado para causar danos a terceiros, envolvendo
sua rede em ataques a outras organizacoes e implicando em um consumo
de banda maior. Alem dessas implicacoes, esse servico pode revelar
informacoes sensiveis sobre sua rede e seus dados armazenados.

Informacoes adicionais sobre como evitar que sua rede seja abusada
para ataques DDoS podem ser encontradas aqui:

https://www.cert.br/docs/whitepapers/ddos/

* Como faco para corrigir o problema?

Em sistemas Microsoft Windows desabilite o recurso chamado NetBIOS sobre TCP/IP (ou NetBIOS over TCP/IP) se ele for desnecessario aos usuarios da rede. Caso nao seja possivel desabilitar esse recurso sugerimos que limite o acesso a este servico apenas para usuarios de sua rede.

Em servidores Unix reconfigure o Samba incluindo a linha abaixo no arquivo de configuracao:

disable netbios = yes

Se o Samba for desnecessario nesse equipamento recomendamos que o desabilite.

* Onde posso obter informacoes adicionais sobre o abuso do protocolo NetBIOS para ataques DDoS?

- UDP-Based Amplification Attacks
https://www.us-cert.gov/ncas/alerts/TA14-017A

- Openly accessible NetBIOS name services
https://www.bsi.bund.de/EN/Topics/IT-Crisis-Management/CERT-Bund/CERT-Reports/HOWTOs/Open-NetBIOS-Nameservices/open-NetBIOS-nameservices_node.html

* Como o CERT.br sabe que este e' um servidor NetBIOS vulneravel?

O CERT.br esta' recebendo notificacoes com listas de servidores NetBIOS que possivelmente estao sendo abusados e utilizados em ataques distribuidos de negacao de servicos (DDoS). O CERT.br esta' notificando os responsaveis pelos servidores brasileiros presentes nestas listas.

* Como posso ter certeza que resolvi o problema?

Voce pode verificar seu servidor atraves do seguinte comando:
(preferencialmente execute-o a partir da Internet, ou seja, fora de uma rede interna que tenha permissao de acesso ao servidor).

A partir de sistemas Microsoft Windows:
$ nbtstat -A IP_SERVIDOR

A partir de sistemas Unix com Samba:
$ nmblookup -A IP_SERVIDOR

Onde IP_SERVIDOR e' o IP do servidor NetBIOS a ser testado.

Se o teste for realizado a partir de um sistema Unix, recomendamos que antes de executar o comando acima certifique-se que voce tem a ferramenta nmblookup instalada em seu computador.

* Onde aprender mais sobre configuracao segura de sistemas?

- Praticas de Seguranca para Administradores de Redes Internet
https://www.cert.br/docs/seg-adm-redes/

* Por que estou recebendo essa mensagem?

Voce esta' recebendo esse email por estar listado em
https://registro.br/ como contato desta rede ou dominio.

Se voce for contato de varias redes diferentes e' possivel que voce
receba mais de um email, com conteudos diferentes. Por favor nao
apague outras copias que vier a receber.

* O que e' o CERT.br?

O CERT.br -- Centro de Estudos, Resposta e Tratamento de Incidentes de
Seguranca no Brasil -- e' o Grupo de Resposta a Incidentes de
Seguranca para a Internet brasileira, mantido pelo NIC.br do Comite
Gestor da Internet no Brasil. E' o grupo responsavel por tratar
incidentes de seguranca em computadores, envolvendo redes conectadas
`a Internet brasileira.