From: cais@cais.rnp.br

Subject: [CAIS #5981463] Host com serviço STUN vulnerável que pode ser utilizado em ataques DDoS [aberto]

Date: 17 August 2024 at 00:46:45 GMT-3

To: deivison@universidadefranciscana.edu.br

Cc: diego.torres@pop-rs.rnp.br, gabriel.zenker@pop-rs.rnp.br, gustavo.dreier@pop-rs.rnp.br, henrison@ufn.edu.br, berthold@pop-rs.rnp.br, estevan@universidadefranciscana.edu.br

Prezado(a),

Segue mensagem que identifica dispositivos com o serviço STUN exposto para internet, que podem ser abusados em ataques DDoS de reflexão UDP e fornecer dados particulares do serviço.

O que é um serviço STUN (Session Traversal Utilities for NAT)?

STUN é uma ferramenta usada por outros protocolos, como o Interactive Connectivity Establishment (ICE), o Session Initiation Protocol (SIP) e o WebRTC. Ele fornece uma ferramenta para os hosts descobrirem a presença de um conversor de endereços de rede e descobrirem o endereço IP mapeado, geralmente público, e o número da porta que o NAT alocou para os fluxos UDP ( User Datagram Protocol ) do aplicativo para hospedeiros remotos.

Solicitamos que as configurações do servidor sejam revistas.

O CAIS recomenda que ao menos uma das soluções abaixo sejam executadas para proteger seus hosts contra ataques desse tipo.

° Caso este dispositivo/serviço não seja utilizado, recomendamos a desativação do mesmo.

° Considere usar STUN sobre TCP por padrão

° Certifique - se restringir o acesso a este serviço para redes conhecidas.

Para verificar se o seu host está vulnerável, execute as rotinas abaixo:

1 - Instalar a ferramenta nmap em uma máquina fora da sua rede

2 - Executar os comandos abaixo (fora da sua rede)

   # nmap -sV -PN -sU -p 3478 --script stun-info <ip\_vulnerável>

Caso o resultado da consulta seja diferente de "OPEN", o seu host não está vulnerável.

Mais informações sobre STUN podem ser encontrados no link:

https://en.wikipedia.org/wiki/STUN

https://www.rfc-editor.org/rfc/rfc5389

https://datatracker.ietf.org/doc/html/rfc8445#section-19.5.1

https://github.com/Phenomite/AMP-Research/tree/master/Port%203478%20(+%20more%20ports)%20-%20STUN

Antes de encerar este incidente junto ao CAIS, certifique-se que:

1.  O incidente foi investigado e identificado:

2.  O incidente foi corrigido, garantindo que ele não voltará a acontecer.

Para encerar o incidente, acesse o sistema SGIS (link abaixo) e atualize o status do incidente:

"https://sgis.rnp.br/incidents/5981463"

O incidente pode também ser encerrado mediante resposta dessa mensagem, conforme segue:

Para incidentes tratados e corrigidos, substitua o campo "Assunto"/"Subject" por:

[CAIS #IDRT] - [RESOLVIDO]

Para incidentes com informações insuficientes ou cujo host denunciado não pertença a Instituição, substitua o campo "Assunto"/"Subject" por:

[CAIS #IDRT] - [CAIS-AJUDA]

Aguardamos seu retorno, certos de sua colaboração, e nos colocamos a disposição para quaisquer esclarecimentos.

Caso você não seja a pessoa apropriada para receber este tipo de mensagem, por favor nos informe a quem devemos contactar para resolver este incidente.

Atenciosamente,

CAIS/RNP

################################################################

#   CENTRO DE ATENDIMENTO A INCIDENTES DE SEGURANCA (CAIS)     #

#       Rede Nacional de Ensino e Pesquisa (RNP)               #

#                                                              #

# cais@cais.rnp.br       https://www.cais.rnp.br/              #

# Tel. 019-37873300      Fax. 019-37873301                     #

# Chave PGP disponivel   https://www.cais.rnp.br/cais-pgp.key  #

################################################################

-----------------------------------------------------------------------------

Data e hora UTC(+0),IP Vulnerável,Porta Origem, Protocolo, Hostname Origem, ASN, Serviço Vulnerável

2024-08-16 00:52:04, 200.132.59.191, 3478, udp, -, 2716, stun

Mais informações:

software: Coturn-4.6.2 'Gorst'

valor da amplificação: 4.40