Redes – EP4

- Titulo (30s) – Arthur
Olá, eu sou o Arthur, E eu e o Lucas estudamos sobre a vulnerabilidade CVE-2020-8794. A vulnerabilidade reside no software OpenSMPTD e através dela é possível executar comandos arbitrários com permissão de super usuário.

- Protocolo SMTP (30s) – Arthur
1) O protocolo SMTP, como vimos em aula, é o protocolo usado entre servidores de e-mail para envio e recebimento de e-mail.

2) Os servidores de e-mail dispõem de uma caixa de entrada, que contém os e-mails recebidos, e uma fila de envio de e-mails que serão enviados.

3) Por fim, o User Agent é a aplicação que atua como cliente de e-mail para acessar e gerenciar o servidor de e-mail.

- OpenSMTPD (30s) – Arthur
O sofware vulnerável é o OpenSMPTD, que é um daemon que implementa o protocolo SMTP para entregar e-mails a uma máquina local ou a outro servidor SMTP.

O OpenSMPTD é um software de código aberto e faz parte do projeto OpenBSD, que é um sistema operacional baseado em UNIX.

- MTA e MDA (30s)
Para entender o cenário em que reside a falha é necessário entender o papel de dois agentes: o MTA e o MDA.
1) O MTA (Message Transfer Agent) é reponsável pelo recebimento de e-mails remotos e pelo envio para outros servidores de e-mail.

2) E o MDA (Message Deliver Agent) é reponsável pelo recebimento de e-mails locais e pela entrega a caixa de entrada.

- Vulnerabilidade - contextualização (1 min)
O OpenSMPTD descreve internamente cada e-mail recebido através de um envelope, que é um arquivo que contém em cada linha um formulário do tipo chave:valor.

Através do envelope, o conteúdo malicioso é injetado no buffer na forma de chave:valor como parte do envelope do e-mail que o MDA está entregando.

A vulnerabilidade se dá devido ao overflow que ocorre no buffer do conteúdo do e-mail e permite a injeção de comandos maliciosos que serão executadas pelo MDA como super usuário.

- Código – em (1 min)

1) A vulnerabilidade se encontra no códido do cliente do OpenSMPTD, no arquivo mta_session.c, mais especificamente na função mta_io(), que é responsável pelo parser do conteúdo do e-mail.

2) A vulnerabilidade ocorre na última linha do e-mail, quando o código SMTP de 3 digítos não é seguido de um espaço opcional e texto e ainda assim o ponteiro aponta para o primeiro caractere após o terminador de string.

3) Neste trecho de código ocorre o parser de cada linha do e-mail a, e no if da última linha da mensagem, onde reside a falha, só é verificado se a linha é vazia.

4) E caso a linha não seja vazia, o ponteiro do buffer é atualizado para apontar após os 3 dígitos e o espaço opcional, permitindo ao attacker injetar o conteúdo malicioso que simula parte do envelope. Esse conteúdo é concatenado a string no método strlcar e depois é copiada ao buffer do conteúdo do e-mail.

5) A vulnerabilidade é passível de ser explorada somente em caso de erro.
Pois nesse caso, a mensagem maliciosa recebida é copiada como valor para a chave "errorline" do envelope do OpenSMPTD. Assim, o attacker utilza o overflow presente no MTA para injetar linhas arbitrarias dentro do envelope do e-mail que o MDA está entregando.

- Lucas
Agora o lucas vai falar sobre o exploit.