Os caos instalado: exploit Log4Shell

Salve jovem padawan, quem diria certas coisas são eternas, reciclam-se, maquiam-se e retornam numa nova roupagem.

O tiozão é da época do Sexta-feira 13, o vírus informático que atormentou todas as empresas do Planeta durante a década de 90.

Um código malicioso, pequenino, quase um ser vivo, afinal foi criado, expandiou-se, em mutação e continuou infectando computadores por muito tempo.

Normalmente um vírus informático explorava falhas de software, obrigando a constantes releases para coibir brechas anteriormente descobertas, as empresas são sempre reativas, nunca preventivas.

Parece a máxima do recall automobilístico, somente é feito, quando o valor a ser pago em indenizações e apólices de seguro forem menores.

Mas voltando ao Log4Shell, ou vírus do Minecraft utiliza uma brecha no software que permite enviar arquivos e através disso dominar a máquina hospedeira, a Microsoft lançou um patch para corrigir

WTF Log4Shell?

Estou imaginando sua cara e respondendo sua pergunta, o que raios um vírus surgido e explorando num popular jogo me afeta?

Afinal as fronteiras são tênues e nunca sabemos o grau de interação entre os softwares, até o momento em que da ruim, justamente foi o que aconteceu com este vírus. A falha explorada existe também em softwares de Cloud, ou seja, os servidores das gigantes da informática são vulneráveis a ele.

Apple, Twitter, Amazon e Google ainda não se pronunciaram a respeito, mas com certeza seus analistas e técnicos estão numa corrida contra o relógio, para atualizar os servidores, bloquear intrusões e descobrir se houve algum ataque.

O restante do mercado esta correndo para atualizarem seus servidores, executando os patchs e rezando para não terem sido afetados, afinal com a LGPD a sanções são dolorosas para o negocio, que tiver dados pessoais furtados.

Nova Zelândia os novos xerifes da WEB?

Mais uma vez, os programadores da Nova Zelandia estão sob os holofotes, afinal desde a entrada do pais no Clube Echolon, o investimento em informática foi maciço, formando uma geração de DEVs habilidosos e os frutos estão sendo colhidos, o LOG4Shell foi amplamente notificado ao mundo por Analistas de Segurança deste pais.

Um pais deve investir em formação e disponibilizar meios para que a comunidade DEV se expanda, veja o grande passo da Digital Innovation One, que disponibiliza cursos gratuitos e atualmente quase 700.000 frequentam a comunidade, estudando, participando dos Bootcamps e Acelerações, publicando artigos no Fórum da Comunidade e interagindo no Discord.

Uma comunidade sadia e vibrante, aprendendo e compartilhando conhecimento, um grupo de programadores, que através da ajuda mutua, solucionando LABs e desafios de código. Aprendendo as melhores práticas do mercado e capacitando uma geração inteira de programadores.

O Brasil está muito atrás na corrida, sofremos com o custo de aquisição de computadores, com preços longe da carteira do comum dos mortais, com o dólar passando dos 6 reais, torna-se mais difícil a atualização dos parque informático e adoção de melhores práticas. Nossa Web de Banda Larga um sonho inatingível para muitas cidades do interior e mesmo bairros nas grandes capitais, aumentam ainda mais o gargalo para os DEVs tupiniquins.

Detalhes do Log4Shell

A falha está num pequeno arquivo em Java utilizado por servidores Apache, que atacou primeiramente os servidores da gigante Alibaba em 24 de Novembro de 2021. Todos os servidores estão expostos e cabe as empresas corrigi-los através do patch.

O exploit  é uma vulnerabilidade RCE de dia zero no aplicativo de log Log4j, uma estrutura de registro Java popular, envolvendo execução arbitrária de código. uma vulnerabilidade de RCE significa que um atacante não precisa ter acesso físico aos computadores para executar um código malicioso, arbitrário que pode levar a um controle completo sobre os sistemas afetados e ao roubo de dados confidenciais, obtendo pontuação máxima na escala CVSS de riscos e vulnerabilidades..

## **O que é CVSS?**

O CVSS, *Common Vulnerability Scoring System,*é um padrão internacionalmente **utilizado para qualificar e avaliar vulnerabilidades presentes nos sistemas informáticos.**

Para entender os reais riscos que cada falha representa foi criado o CVSS, um **método usado para classificar o risco das vulnerabilidades presentes em algum *software* através de uma pontuação numa escala de 0 a 10, conheça o nível de gravidade, na tabela abaixo:**

* Entre 0,0 e 3,9: Baixo;
* Entre 4,0 e 6,9: Médio;
* Entre 7,0 e 10,0: Alto.

Os danos são calculados de acordo com a métrica a seguir.

* **Potencial Dano Colateral:**potencial de furto ou danificação dos [dados](https://ecoit.com.br/protecao-de-dados-pessoais/);
* **Distribuição de Destinos:**número de sistemas no ambiente que podem ser usados como destinos;
* **Requisito de Disponibilidade:**importância  da disponibilidade das informações;
* **Requisito de Confidencialidade:**importância da confidencialidade das informações;
* **Requisito de Integridade:**importância da precisão das informações.

**Fogo no palheiro**

**Com a publicação e liberação do script em inúmeros fóruns de crackers, noobs e** *script kiddies’* (jovens hackers inexperientes) estão testando todos os servidores existentes em busca de vantagem.

Recomenda-se vivamente a atualização de segurança e instalação dos patchs para proteger seus equipamentos e dados sensíveis de clientes, bem como backups e monitoramento do trafego.

O triste é que muitos garotos nem sabem o que estão fazendo, seguindo passo a passo os tutoriais do mal, conseguem acesso aos computadores e a anarquia instala-se, grafitando páginas, instalando outros vírus, roubando dados pessoais e descabelando o boneco, numa balburdia que arrancam os cabelos dos Admins.

A importância do teste de software

Atualmente as empresas sentem a necessidade de lançar releases e mais releases, mas essa pressa acaba deixando muitos trechos com bugs e vulnerabilidades não testadas.

Quando são descobertas o caos se instala, gerando muita dor de cabeça e perdas financeiras em escala global. Por isso nós que somos DEVs, devemos sempre nos esforçar ao máximo para proteger nossos clientes, testando e garantindo a segurança do software entregue.

Conclusão,

Caro padawan infelizmente entra ano, sai ano, mas algumas coisas são constantes, softwares com bugs e anomalias, administradores de servidores negligentes e preguiçosos.

A desídia causa mais danos que o próprio exploit, é de longa data os aprendizes de hackers, que utilizam-se de receitas de bolo compartilhadas vezes sem conta em fóruns na Deep Web para obterem vantagens e explorarem RCEs em falhas D0.