Tempest

Política de Divulgação Coordenada de Vulnerabilidades

1. Objetivo

Esta política tem o objetivo de disciplinar o processo de divulgação de vulnerabilidades de segurança.

2. Escopo

A política abrange as vulnerabilidades identificadas em qualquer tipo de tecnologia, incluindo tecnologias desenvolvidas pela Tempest.

3. Princípios

Esta política visa atender a um conjunto de princípios os quais a Tempest considera como valores intrínsecos ao processo de descoberta e divulgação de vulnerabilidades. São eles:

3.1. Na Tempest a busca por vulnerabilidades é orientada pelo desejo de trazer mais segurança para os clientes e para a sociedade.

3.2. As entidades devem buscar o diálogo para divulgar vulnerabilidades de modo responsável.

3.3. Os recursos e esforços para encontrar vulnerabilidades precisam ser proporcionais a provar que a vulnerabilidade existe.

3.4. A definição das regras para a divulgação coordenada de vulnerabilidades traz equilíbrio no relacionamento entre as entidades do processo e protege os pesquisadores.

3.5. A divulgação de vulnerabilidades à revelia do fabricante (full disclosure) é orientada pelo benefício à sociedade em condições nas quais há perigo iminente de sua exploração. Este tipo de divulgação somente pode ocorrer em situações nas quais todas as tentativas de comunicação ou consenso entre as partes tenham se esgotado até o prazo limite determinado no item 7.1.7 abaixo.

4. Definições

Vulnerabilidade – é um conjunto de condições ou comportamentos que possibilitam a violação de uma política de segurança explícita ou implícita. Vulnerabilidades podem ser causadas por defeitos de software, decisões sobre configuração ou design, interações inesperadas entre sistemas ou mudanças no ambiente. A exploração bem-sucedida de uma vulnerabilidade possui impactos técnicos e de risco. Vulnerabilidades podem surgir em sistemas de processamento de informações tão cedo quanto em fase de projeto e tão tarde quanto na implantação do sistema.

Risco – Uma medida da extensão em que uma entidade é ameaçada por uma circunstância ou evento em potencial, é tipicamente uma função de: (i) os impactos adversos que surgiriam se a circunstância ou evento ocorresse; e (ii) a probabilidade de ocorrência.

Impacto Potencial – A perda de confidencialidade, integridade ou disponibilidade que se pode esperar causando um efeito adverso limitado, grave ou catastrófico sobre operações e ativos organizacionais ou indivíduos.

CVSS – acrônimo para Common Vulnerability Scoring System – Sistema Comum de Pontuação de Vulnerabilidade, em uma tradução livre. Trata-se de uma maneira de capturar as principais características de uma vulnerabilidade e lhe dar uma nota de acordo com sua severidade, o que pode ajudar as organizações a priorizar atividades de correção da falha de acordo com seu impacto potencial e risco.

CVD – acrônimo para Coordinated Vulnerability Disclosure – Divulgação Coordenada de Vulnerabilidade. Consiste em um processo para a redução da vantagem de adversários enquanto uma vulnerabilidade de segurança da informação é mitigada. CVD é um processo, não um evento. Liberar um patch ou publicar um documento são eventos importantes dentro do processo, mas não o definem.

5. Papéis e Responsabilidades

Por ser um processo coordenado, o CVD pode envolver múltiplas organizações, tais como empresas, fundações, agências governamentais e indivíduos, os quais podem assumir diversos papéis e responsabilidades específicas no processo. A Tempest pode, por exemplo, assumir o papel de finder de relator e coordenador para as vulnerabilidades que encontra. Adicionalmente pode também assumir o papel de fabricante e deployer para as vulnerabilidades encontradas em suas teconologias.

Finder – indivíduo ou organização que encontra a vulnerabilidade. Muitas vezes se trata de um pentester ou pesquisador de segurança os quais estão motivados pelo desafio técnico ou pelo reconhecimento que a divulgação da vulnerabilidade pode oferecer. Eventualmente essa função é desempenhada institucionalmente por empresas ou pelo próprio fabricante.

Relator – indivíduo ou organização que comunica a vulnerabilidade ao fabricante. Em muitos casos essa atividade é desempenhada pelo Finder. Entretanto, a atividade pode ser eventualmente desempenhada por uma empresa que intermedeia a comunicação entre o fabricante e o Finder, cobrando uma taxa sobre a recompensa atrelada à divulgação responsável do problema.

Fabricante – Empresa, organização sem fins lucrativos, agência governamental, indivíduo ou grupo de indivíduos que cria, desenvolve e/ou mantém tecnologias. No CVD esta é a entidade responsável por avaliar a documentação enviada pelo Finder, planejar e desenvolver correções, bem como disponibilizá-las para os Deployers.

Deployer – Indivíduo ou organização com a função de planejar, testar e implementar correções para vulnerabilidades.

Coordenador – Indivíduo ou área em uma organização com a função de gerir o ciclo de identificação de correção de vulnerabilidades no processo de CVD. Eventualmente o processo pode demandar a coordenação de atividades entre múltiplas empresas o que acarreta em um coordenador para todo o caso. Na Tempest, essa função é ocupada por funcionários com o badge de Research Advisor.

6. Fases do CVD

Descoberta – momento em que a vulnerabilidade é identificada. Isto pode acontecer acidentalmente ou dentro do escopo de uma pesquisa.

Reporting – momento em que o Finder e/ou o Relator documentam a descoberta da vulnerabilidade em um "vulnerability advisory".

Validação e Triagem – momento em que o fabricante valida a acurácia da documentação e prioriza essa correção em relação a outras possíveis atividades semelhantes.

Remediação – atividade de desenvolver uma correção para o problema e testá-la.

Deployment – fase em que o Deployer planeja, testa e implementa a correção em seu ambiente.

7. Diretrizes

Com as diretrizes abaixo, a Tempest busca aplicar um conjunto de regras gerais para o tratamento de vulnerabilidades, tanto as identificadas em suas soluções, quanto às que encontra nas mais variadas tecnologias.

Essa iniciativa, se baseia em práticas reconhecidas internacionalmente e possui o objetivo de contribuir para a segurança de todos, conforme detalhado na seção 3 "princípios" deste documento. Portanto, a Tempest cumpre com as diretrizes dessa política e espera que as outras organizações também estejam em conformidade com ela.

7.1. Diretrizes do Coordenador

7.1.1. O coordenador deve agir sob as princípios dessa política;

7.1.2. O coordenador opera como um gerente de projetos, resolvendo conflitos e desobstruindo o canal de comunicação entre todas as partes;

7.1.3. Toda comunicação do Coordenador com as partes deve acontecer por canais criptografados;

7.1.4. Quando na situação em que a vulnerabilidade envolva múltiplos fabricantes é conveniente os representantes de todas as organizações envolvidas elegerem um coordenador exclusivo para o projeto;

7.1.5. Os detalhes da divulgação serão negociados pelo coordenador com todas as partes. Se múltiplas organizações estiverem envolvidas, a divulgação só poderá acontecer quando todas concordarem.

7.1.6. O coordenador deverá negociar com o fabricante uma data limite para a divulgação da vulnerabilidade a qual, a princípio, não deve ser superior a 90 dias a contar da primeira comunicação entre as partes.

7.1.7. Casos em que não há cooperação do fabricante, ou em que este não considere a situação como uma vulnerabilidade, devem ser submetidos ao diretor do coordenador para que a publicação à revelia seja deliberada pela gestão.

7.2. Diretrizes do Finder

7.2.1. O Finder deverá reportar a vulnerabilidade inicialmente ao coordenador, se houver pessoa com essa função.

7.2.2. O Finder é responsável por seus atos e deve estar ciente de que reportar a vulnerabilidade não o absolve de uma investigação criminal, caso este tenha usado a vulnerabilidade para finalidades criminosas;

7.2.3. O Finder deve reportar a vulnerabilidade o mais rápido possível para minimizar o risco de exploração maliciosa;

7.2.4. Toda comunicação do Finder com as partes precisa acontecer preferencialmente por canais criptografados;

7.2.5. Na ausência do Relator, o Finder deve reportar a vulnerabilidade seguindo os critérios definidos na seção 7.3, abaixo;

7.2.6. Suas ações devem ser proporcionais a provar que a vulnerabilidade existe, evitando;

Usar engenharia social para obter acesso ao sistema;

Criar seu próprio backdoor no sistema com a intenção de demonstrar a vulnerabilidade, pois assim poderia criar dano adicional ou gerar riscos desnecessários;

Utilizar a vulnerabilidade mais tempo que o necessário para estabelecer a sua existência;

Copiar, modificar ou deletar dados no sistema;

Enumerar ou fazer lista dos diretórios do sistema;

Modificar o sistema;

Obter acesso repetidamente ao sistema;

Compartilhar seu acesso ao seu sistema com outras pessoas;

Usar técnicas de brute force para obter acesso ao sistema.

7.3. Diretrizes do Relator

7.3.1. O Relator deverá construir o Vulnerability Advisory contemplando as seguintes informações sobre vulnerabilidade:

Versão do documento;

Data da primeira versão do advisory e da versão atual;

CVSS da vulnerabilidade e sua descrição;

Qual a tecnologia vulnerável;

Qual a versão – ou versões – vulneráveis;

Qual é o tipo de vulnerabilidade;

Qual é o impacto potencial da exploração bem-sucedida da vulnerabilidade;

Quais são as situações adversas da exploração malsucedida da vulnerabilidade. Exemplo: casos em que a execução do exploit resulta em erro, porém causa negação de serviço no alvo;

Descrição dos recursos necessários e condições pré-existentes para o ataque ocorrer.

Possíveis soluções de contorno que evitam a exploração da vulnerabilidade.

Evidências técnicas que comprovem que a vulnerabilidade é passível de exploração.

7.3.2. Toda comunicação do Relator com as partes precisa acontecer por canais criptografados.

7.4. Diretrizes do fabricante

7.4.1. O fabricante se compromete a manter canais para que Finders e relatores possam comunicar a empresa sobre vulnerabilidades em seus produtos;

7.4.2. O fabricante se compromete a não estabelecer limites para a comunicação sobre vulnerabilidades;

7.4.3 O fabricante deve contar com pessoas qualificadas para responder a qualquer comunicação sobre vulnerabilidades em seus produtos;

7.4.4. A empresa deve garantir que, ao receber um vulnerability advisory, este será enviado o mais rápido possível para o grupo com mais condições de respondê-lo;

7.4.5. O grupo incumbido de tratar o vulnerability advisory deverá enviar uma confirmação de recebimento ao Finder e/ou relator, assim que receber o documento, preferencialmente assinada digitalmente;

7.4.6. Convém que o fabricante apresente uma correção para a vulnerabilidade em até 90 dias;

7.4.7. O tempo para a apresentação de uma correção pode ser reduzido ou aumentado de acordo com a criticidade e/ou complexidade do problema;

7.4.8. O fabricante deverá comunicar o Finder, o relator e/ou o coordenador sobre o status de cada atividade de correção;

7.4.9. O fabricante pode optar por bonificar o Finder pela descoberta da vulnerabilidade;

7.4.10. O fabricante pode optar por divulgar a vulnerabilidade antecipadamente a seus parceiros ou grupos de interesse;

7.4.11. A iniciativa de oferecer uma recompensa pelo reporte de vulnerabilidades é exclusiva da organização, a qual pode determinar as condições para isso em uma política pública.

7.4.12. Por aceitar os termos da política de divulgação coordenada de vulnerabilidades, o fabricante declina de tomar ações legais contra os pesquisadores que descobriram a vulnerabilidade. A não ser que uma investigação criminal comprove que estes usaram a vulnerabilidade para finalidades criminosas.

8. Referências

Software Vulnerability Disclosure in Europe:Technology, Policies and Legal Challenges.CEPS Task Force. Junho de 2018.

The CERT® Guide to Coordinated Vulnerability Disclosure. CERT Division. Carnegie Mellon University. August 2017.

NIST Special Publication 800-30: Guide for Conducting Risk Assessments.National Institute of Standards and Technology. September 2012.

NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. National Institute of Standards and Technology. April 2013.

FIPS PUB 200: Minimum Security Requirements for Federal Information and Information Systems.National Institute of Standards and Technology. 9 March 2006.

Economics of vulnerability disclosure. ENISA. December 2018.