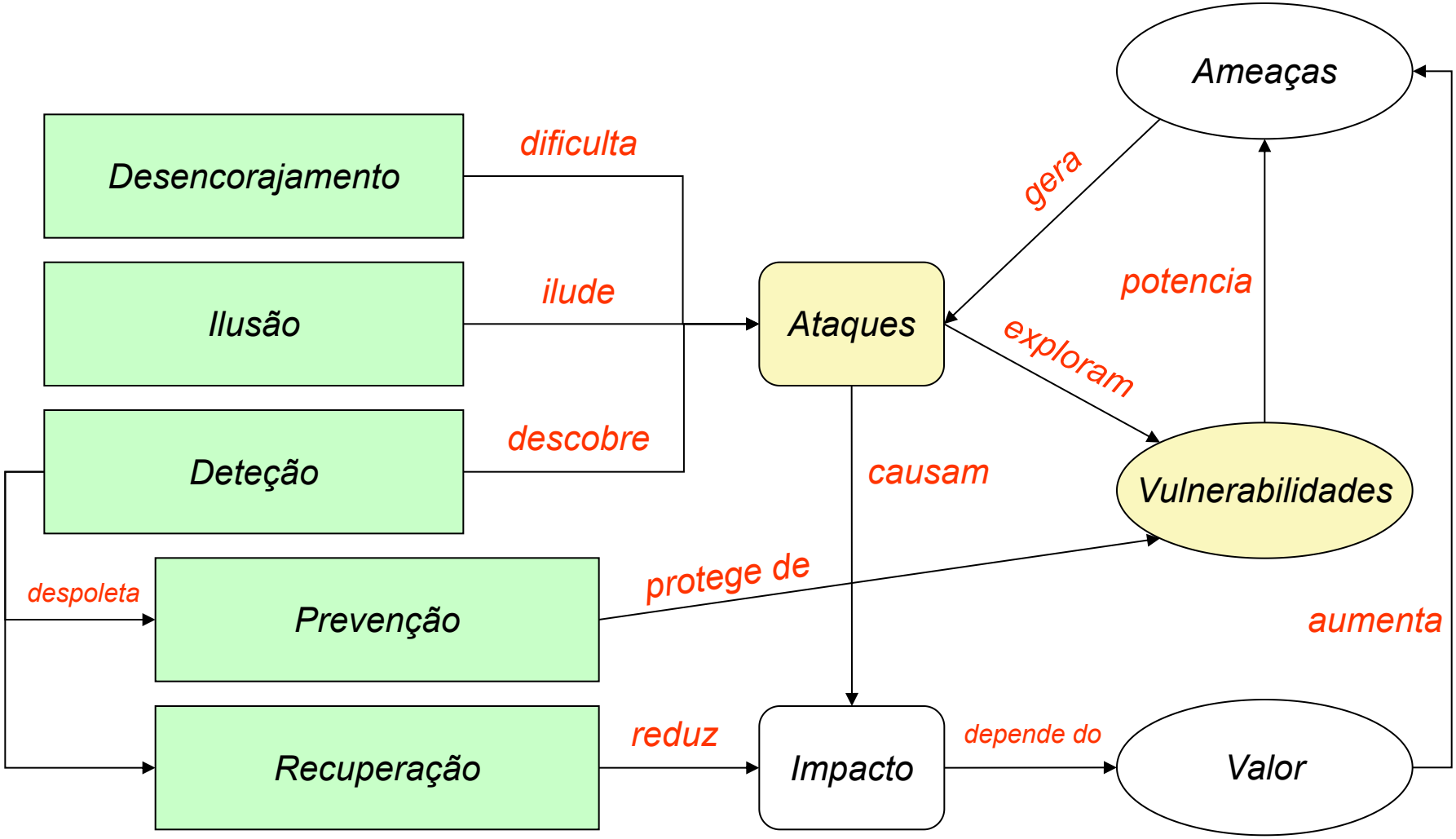
Vulnerabilidades

Segurança da Informação



Medidas (e algumas ferramentas)

- **Desencorajamento**
  - Punição
    - Restrições legais
    - Provas forenses
  - Barreiras de Segurança
    - Firewalls
    - Autenticação
    - Comunicação Segura
    - Sandboxing
- **Deteção**
  - Sistemas de Deteção de Intrusões
    - ex: Snort, Zeek, Suricata
  - Auditorias
  - Análise Forense
- **Ilusão**
  - Honeypots /Honeynets
  - Acompanhamento Forense
- **Prevenção**
  - Políticas restritivas
    - ex: privilégio mínimo
  - Deteção de vulnerabilidades
    - ex: OpenVAS, metasploit
  - Correção de Vulnerabilidades
    - ex: atualizações regulares
- **Recuperação**
  - Backups
  - Sistemas redundantes
  - Recuperação forense

Prontidão (Security Readiness)

- **Medidas de Desencorajamento, Ilusão e Deteção endereçam maioritariamente vulnerabilidades conhecidas**
  - Tentativas de reconhecimento (ex: Port Scanning)
  - Ataques genéricos (ex: Interceção de redes)
  - Ataques específicos (ex: Buffer Overflows)

- **Medidas de Prevenção endereçam vulnerabilidades conhecidas e desconhecidas**
  - Vulnerabilidades genéricas
    - ex: reação a respostas mal formadas (protocol scrubbers)
    - ex: ataques furtivos (normalização para formatos canónicos)
  - Vulnerabilidades específicas
    - ex: erro de particular de software (testes e validação)

Prontidão (Security Readiness)

A aplicação das medidas requer conhecimento específico

- **Vulnerabilidades conhecidas**
  - Problema, forma de exploração, impacto, etc
- **Padrões de atividade dos ataques**
  - Modus operandi
  - Assinaturas de ataques
- **Padrões anormais de atividade**
  - Anormal é o oposto de normal…
  - … mas o que é que é normal?
  - Difícil de definir em ambientes heterogéneos

source: flickr

Prontidão (Security Readiness)

- **As ameaças em redes de computadores são diferentes de outros tipos de ameaças**
  - Os ataques podem ser lançados em qual hora, de qualquer local
  - Podem ser facilmente coordenados
    - e.g. Distributed Denial of Service attacks (DDoS)
  - São baratos
  - Podem ser automatizados
  - São rápidos

- **Portanto, requerem uma capacidade permanente (24x7) de reação a ataques:**
  - Equipas de especialistas em segurança
  - Alertas de ataque na hora
  - Teste e avaliação dos níveis de segurança existentes
  - Procedimentos de reação expeditos

Ataques de dia Zero (0 day)

- **Ataque que usa vulnerabilidades que são**
  - Desconhecidas de terceiros
  - Não comunicadas ao fornecedor de software
- **Ocorre no dia zero do conhecimento dessas vulnerabilidades**
  - Para as quais não existe correção (ou não está aplicada)
- **Um ataque "0 day" pode existir por meses/anos**
  - Conhecido para atacantes mas não para utilizadores
  - Parte frequente de arsenais de ataques informáticos
  - Comercializados em mercados específicos

ShadowBrokers

- **Background: Atores estatais possuem arsenal para explorar vulnerabilidades desconhecidas do público**
  - Parte integrante das suas atividades, por muitos ano e nunca reveladas
- **Agosto 2016: Shadowbrokers publicam um grande quantidade de ferramentas deste atores**
  - Usando canais públicos: Twitter, Github, PasteBin, Medium
  - Apresentam outros conjuntos de ferramentas: fazem um leilão, fazem uma venda de Black Friday, etc...
  - Objetivo: vender ferramentas que exploram 0 days a quem pagar mais
- **Março 2017: Microsoft lança atualizações para várias versões de Windows**
  - mas não lança para o W7, W8, XP e Server 2003
  - poderá ter existido dica de investigadores ou atores estatais
  - gravidade da atualização não é realçada

ShadowBrokers

- **Abril 2017: ETERNALBLUE libertada ao público num dos pacotes**
  - Explora vulnerabilidade no MS Windows SMB v1 (Remote Code Execution)
- **Maio 2017: Wannacry ransomware**
  - Utiliza 2 exploits libertados pelos SB (ETERNALBLUE é o 1º)
  - Impacto: Cifra ficheiros, afeta > 300K dispositivos
  - Pede resgate de $300-$600 para obtenção da chave de decifra
- **Maio 2017: EternalRocks ransomware**
  - Utiliza 7 exploits libertados pelos SB (ETERNALBLUE é o 1º)
  - Impacto: Pânico apenas. Autor desativa ataque
- **Junho 2017: NotPetya ransomware**
  - Variante que utiliza ETERNALBLUE e cifra ficheiros
  - Pede resgate de $300 (mas não é possível decifrar ficheiros)
  - Alvo: Infraestruturas críticas, bancos, jornais na Ucrânia e Rússia (outros tb afetados)
  - Impacto: Ficheiros perdidos, >$10B de danos


If you see this text, then your files are no longer accessible, bec
have been encrypted. Perhaps you are busy looking for a way to rec
files, but don't waste your time. Nobody can recover your files wi
decryption service.
We guarantee that you can recover all your files safely and easily.
need to do is submit the payment and purchase the decryption key.
Please follow the instructions:
1. Send $300 worth of Bitcoin to following address:
1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX
2. Send your Bitcoin wallet ID and personal installation key to e-m
wowsmith123456@posteo.net. Your personal installation key:
X86Gc2-7PRNBE-3mNFMp-z88VnG-uF5nhF-4wzxw2-XdNrr6-FYG89D-xk4rNz-9


Wana Decrypt0r 2.0
Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
1/3/1970 17:00:00
Time Left
00:00:00:00
Your files will be lost on
1/7/1970 17:00:00
Time Left
00:00:00:00
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin ACCEPTED HERE
Send $600 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw
Copy
Check Payment
Decrypt

Deteção de Vulnerabilidades

- **Ferramentas específicas podem detetar vulnerabilidades**
  - Exploram vulnerabilidades conhecidas
  - Testam padrões de vulnerabilidades
  - ex. buffer overflow, SQL injection, XSS, etc.
- **Ferramentas específicas podem replicar ataques conhecidos**
  - Utilizam exploits conhecidos para vulnerabilidades conhecidas
    - ex: MS Samba v1 utilizado no WannaCry
  - Permitem implementar correções mais rapidamente
- **Vitais para aferir a robustez das aplicações e sistemas em operação**
  - Serviço frequentemente contratado

Deteção de Vulnerabilidades

- **Podem ser aplicadas a:**
  - Código desenvolvido (análise estática)
    - OWASP LAPSE+, RIPS, Veracode, …
  - Aplicação a executar (análise dinâmica)
    - Valgrind, Rational, AppScan, GCC, …
  - Externamente como um sistema remoto
    - OpenVAS, Metasploit, …
- **Não devem ser aplicadas de forma cega a sistemas em produção!**
  - Potencial perda/corrupção de dados
  - Potencial negação de serviço
  - Potencial ato ilegal

Sobrevivência

Como se sobrevive a uma ataque do dia zero?

Como se reage a uma ataque do dia zero massivo?

- **Diversidade poderá ser uma solução …**
  - Mas a produção, distribuição e atualização de software vai no sentido contrário!
    - E o mesmo acontece com as arquiteturas de hardware
  - Porque é que o MS Windows é um alvo primordial?
    - E o MAC OS nem por isso?
  - Está a usar um telemóvel Android?
    - Qual é a probabilidade de estar na linha da frente das vítimas?
    - iOS pode ser pior, pois o ecossistema é ainda mais homogéneo

CVE: Common Vulnerabilities and Exposures

- **Dicionário público de vulnerabilidades e exposições de segurança**
  - Para gestão de vulnerabilidades
  - Para gestão de correções (patches)
  - Para alarmística de vulnerabilidades
  - Para deteção de intrusões
- **Utiliza identificadores comuns para um mesmo CVE**
  - Permite a troca de informações entre produtos de segurança
  - Fornece uma base de indexação para avaliar a abrangência de ferramentas e serviços
- **Detalhes de um CVE podem ser privados**
  - Parte do processo de divulgação responsável: espera-se que o fornecedor crie uma correção

CVE: Vulnerabilidade

Erro no software que pode ser usado diretamente por um atacante para ganhar acesso ao sistema ou à rede

- **Um erro só é uma vulnerabilidade se permitir que o atacante viole uma política de segurança**
  - Exclui políticas de segurança "abertas" onde todos os utentes são de confiança ou onde não se considera a existência de riscos para o sistema

- **Um vulnerabilidade é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente permite:**
  - que um atacante execute comandos em nome de terceiros
  - que um atacante aceda a dados ultrapassando as restrições de acesso
  - que o atacante se apresente como outrem
  - que o atacante negue a prestação de serviços

CVE: Exposição

Problema de configuração de um sistema ou um erro no software que permitem aceder a informação ou capacidades que podem auxiliar um atacante

- **O CVE considera um problema de configuração ou um erro como uma exposição se não permitir comprometer diretamente um sistema ou rede**
  - Mas for uma componente importante para o sucesso de um ataque e uma violação de uma política de segurança expectável

- **Uma exposição é um estado de um sistema computacional (ou conjunto de sistemas) que, alternativamente:**
  - permite que um atacante realize recolhas de informação
  - permite a um atacante esconder as suas atividades
  - Inclui uma funcionalidade que se comporta como esperado mas que pode ser facilmente comprometida
  - É um ponto de entrada comum para atacantes obterem acesso (a sistemas ou dados)
  - É considerado problemático por uma política de segurança razoável

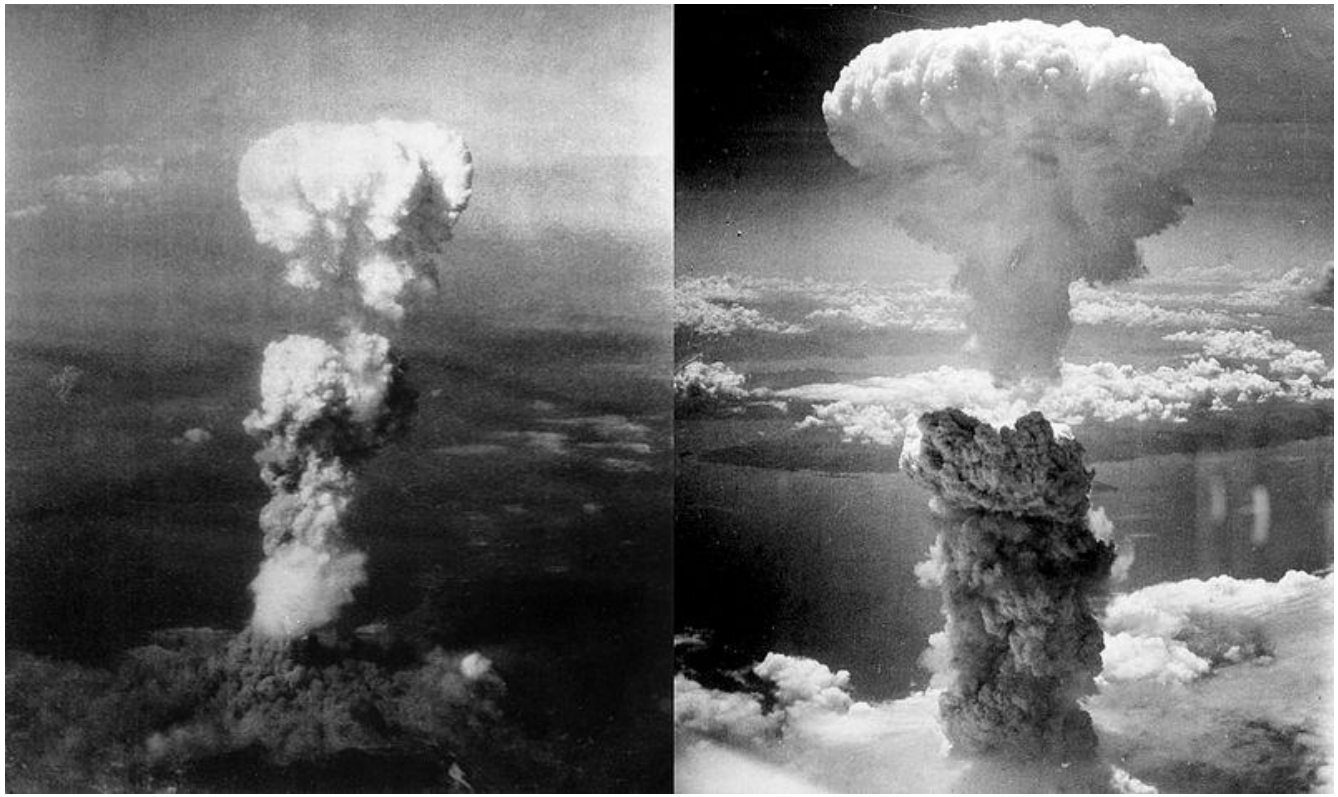
Benefícios dos CVEs

Fornece uma linguagem comum para referir problemas

- **Facilita a partilha de dados entre**
  - Sistemas de deteção de intrusões
  - Ferramentas de aferição
  - Bases de dados de vulnerabilidades
  - Investigadores
  - Equipas de resposta a incidentes
- **Permite melhorar as ferramentas de segurança**
  - Maior abrangência, facilidade de comparação, interoperabilidade
  - Sistemas de alarme e reporte
- **Fomenta a inovação**
  - Local primordial para discutir conteúdos críticos das BDs

Limitações dos CVEs

Inúteis contra ataques de dia zero



CVE: Identificadores

Aka CVE names, CVE numbers, CVE-IDs, or CVEs

- **Identificadores únicos para vulnerabilidades conhecidas e públicas da CVE List**
  - Estados possíveis: "candidate" ou "entry"
  - **Candidate**: sob revisão para inclusão na CVE List
  - **Entry**: aceite na CVE List
- **Formato**
  - Identificador numérico CVE (CVE-Ano-Índice)
  - Estado (candidate ou entry)
  - Descrição sumária da vulnerabilidade ou exposição
  - Referências para informação adicional

CVEs e Ataques

- **Ataques podem usar várias vulnerabilidades**
  - Um CVE para cada vulnerabilidade em todos os sistemas

- **Exemplo: Stagefright (Android, video em mensagens MMS)**
  - CVE-2015-1538, P0006, Google Stagefright ‘stsc’ MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1538, P0004, Google Stagefright ‘ctts’ MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1538, P0004, Google Stagefright ‘stts’ MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1538, P0004, Google Stagefright ‘stss’ MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-1539, P0007, Google Stagefright ‘esds’ MP4 Atom Integer Underflow Remote Code Execution
  - CVE-2015-3827, P0008, Google Stagefright ‘covr’ MP4 Atom Integer Underflow Remote Code Execution
  - CVE-2015-3826, P0009, Google Stagefright 3GPP Metadata Buffer Overread
  - CVE-2015-3828, P0010, Google Stagefright 3GPP Integer Underflow Remote Code Execution
  - CVE-2015-3824, P0011, Google Stagefright ‘tx3g’ MP4 Atom Integer Overflow Remote Code Execution
  - CVE-2015-3829, P0012, Google Stagefright ‘covr’ MP4 Atom Integer Overflow Remote Code Execution

CVE-2015-1538

CVE-ID	
CVE-2015-1538	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings

Description

** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

Date Entry Created	
20150206	Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20150206)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE list, which standardizes names for security problems.

SEARCH CVE USING KEYWORDS: Submit

You can also search by reference using the CVE Reference Maps.

For More Information: cve@mitre.org

U C
S A
E S
E

CVE-ID

CVE-2015-1538 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Integer overflow in the SampleTable::setSampleToChunkParams function in SampleTable.cpp in libstagefright in Android before 5.1.1 LMY48I allows remote attackers to execute arbitrary code via crafted atoms in MP4 data that trigger an unchecked multiplication, aka internal bug 20139950, a related issue to CVE-2015-4496.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BID:76052
- URL:http://www.securityfocus.com/bid/76052
- CONFIRM:http://www.huawei.com/en/psirt/security-advisories/hw-448928
- CONFIRM:http://www1.huawei.com/en/security/psirt/security-bulletins/security-advisories/hw-448928.htm
- CONFIRM:https://android.googlesource.com/platform/frameworks/av/+/2434839bbd168469f80dd9a22f1328bc81046398
- EXPLOIT-DB:38124
- URL:https://www.exploit-db.com/exploits/38124/
- MISC:http://packetstormsecurity.com/files/134131/Libstagefright-Integer-Overflow-Check-Bypass.html
- MLIST:[android-security-updates] 20150812 Nexus Security Bulletin (August 2015)
- URL:https://groups.google.com/forum/message/raw?msg=android-security-updates/Ugvu3fi6RQM/yzJvoTVrIQAJ
- SECTRACK:1033094
- URL:http://www.securitytracker.com/id/1033094

Assigning CNA

MITRE Corporation

Date Entry Created

20150206 Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20150206)

Votes (Legacy)

Comments (Legacy)

Proposed (Legacy)

N/A

This is an entry on the CVE List, which provides common identifiers for publicly known cybersecurity vulnerabilities.

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

For More Information: CVE Request Web Form (select "Other" from dropdown)

CWE: Common Weakness Enumeration

- **Linguagem comum para discutir, encontrar e lidar com as causas das vulnerabilidades de segurança**
  - De programas, do seu desenho ou da arquitetura de sistemas
  - Cada CWE representa um tipo de vulnerabilidade
  - Gerida pela MITRE Corporation
    - Uma lista de CWE é disponibilizada pela MITRE
  - Esta lista fornece uma definição pormenorizada de cada CWE

- **Os CWEs são catalogados segundo uma estrutura hierárquica**
  - CWEs localizados nos níveis superiores fornecem uma descrição genérica sobre o tipo de vulnerabilidade
    - Podem ter vários CWEs filhos associados
  - CWEs nos níveis inferiores descrevem problemas de uma forma mais focada
    - Com menos ou sem CWEs filhos

CWE != CVE

K. Teipenyuk, B. Chess, & G. McGraw
Seven Pernicious Kingdoms: A Taxonomy of Software Security Errors
IEEE Security & Privacy, 2005

1. **Validação e representação de entradas**
2. **Abuso de API:** falhas na utilização de interfaces
3. **Funcionalidades de segurança:** más práticas
4. **Tempo e estado:** threads, concorrência
5. **Erros:** má geração ou recuperação
6. **Qualidade do código**
7. **Encapsulamento**
8. ***Ambiente de execução:** configurações e características

https://cwe.mitre.org/data/definitions/700.html

CERT: *Computer Emergency Readiness Team*

- **Organização para garantir que as praticas de gestão de tecnologias e sistemas são usadas para:**
  - Resistir a ataques em sistemas distribuídos (em rede)
  - Limitar o dano, garantir a continuidade de serviços críticos
  - Mesmo considerando ataques realizados com sucesso, acidentes e falhas
- **CERT/CC (Coordination Center) @ CMU**
  - Um componente do CERT Program
  - Um hub para questões de segurança na Internet
  - Criado em Novembro 1988 depois do "Morris Worm”
  - Tem demonstrado a crescente exposição da Internet a ataques

CSIRT: *Computer Security Incident Response Team*

- **Organização responsavel por receber, rever e responder a relatórios de incidentes e atividade**
  - Fornece serviço 24/7 para usuários, companhia, agências governamentais e organizações
  - Fornece um ponto único de contato fiável e confiável para reportar incidentes de segurança à escala global
  - Fornecem os meios para reportar incidentes e disseminar informação relativa a incidentes

- **CSIRTs Nacionais**
  - CERT.PT: https://www.facebook.com/CentroNacionalCibersegurancaPT
  - National CSIRT Network: https://www.redecsirt.pt
  - CSIRT @ UA: https://csirt.ua.pt

Alertas de segurança & Tendências de atividades

- **Vitais para a disseminação rápida de conhecimento sobre novas vulnerabilidades**
  - US-CERT Technical Cyber Security Alerts
  - US-CERT (non-technical) Cyber Security Alerts
  - SANS Internet Storm Center
    - Aka DShield (Defense Shield)
  - Microsoft Security Response Center
  - Cisco Security Center

  - E muitos outros

Regras Importantes

Endereçar a segurança como um todo

- **Considerar frameworks existentes (ISO 27001, 27002)**
  - melhores práticas e recomendações
- **Considerar requisitos normativos**
  - adicionar verificações de risco e estratégias de resolução
- **Considerar os aspetos legais**
  - Leis a obedecer, regulamentos, questões contratuais
- **Criar controlos e garantir que estes endereçam os requisitos**
- **Avaliar o funcionamento do programa de segurança**

Regras Importantes

Identificar e Gerir o Risco

- **Considerar o risco específico para sistema/negócio/operações**
  - Ter em conta os aspetos operacionais, tecnologia em utilização
  - Ter em conta os dispositivos e interações com terceiros
    - ex: pagamentos com cartões
- **Identificar o risco em todas as áreas da organização**
  - tecnologia, relações com terceiros, pessoas
- **Definir medidas preventivas para reduzir o risco**
  - Considerar o ataque e o impacto na organização
- **Avaliar periódicamente o risco**

Regras Importantes

Seguir a informação

- **Informação contém valor**
  - Atacantes: Ataques focam-se em áreas com maior valor
  - Regulamentar: Fugas podem implicar multas altas
  - Negócio: Fugas/manipulações podem implicar perdas elevadas
- **Conhecer bem onde está a informação em cada momento**
  - Quem a manipula
  - Onde é armazenada
  - Por onde circula
- **Classificar informação de acordo com risco/visibilidade**
  - confidencial, privada, pública, dados pessoais

Regras Importantes

Aplicar medidas de defesa em profundidade

- **A superfície de ataque é extensa**
  - Adversário externos, ou que ganhem acesso interno
  - Colaboradores
- **Garantir que existem controlos adequados e suficientes**
  - Conciliar deteção de fugas/manipulação e alteração
  - Considerar colaboradores, terceiros, público em geral
- **Considerar também métodos físicos**
  - Air Gaps, Portas, infraestruturas
- **Aplicar requisitos de segurança na linguagem da organização**

Regras Importantes

Alinhar a segurança com objetivos, produtos, serviços

- **Mandatório para garantir que a segurança acompanha a organização**
  - Continua relevante, existe e tem impacto
- **Evoluir da simples proteção do que é obrigatório**
  - Considerar todos os dados
- **Ter conhecimento de como a organização opera, produtos são desenvolvidos/vendidos/operados**
  - Saber como aplicar a segurança
- **Ter conhecimento da geração de lucro**
  - Saber como calcular o impacto de um ataque

Regras Importantes

Antecipar, Inovar e Adaptar

- **Ataques, negócio e vulnerabilidades evoluem**
  - Necessário que a segurança acompanhe a evolução
  - Seguir CSIRTS, CERTs, etc...
- **Foco nos pontos onde existe um maior retorno da proteção**
  - O que é mais fácil de proteger
  - O que possui maior dano (e é razoável de ser efetuado)
- **Considerar ataques persistentes avançados (APT)**
  - Não acontecem só “aos grandes”

Regras Importantes

Estabelecer uma cultura baseada na segurança

- **Fornecer formação aos colaboradores**
  - Para entenderem os riscos, impacto e mitigações
  - Para conhecerem as boas práticas, mecanismos e soluções
  - Que seja apoiada e aplicada em todos os níveis hierárquicos
- **Construir políticas que se apliquem a toda a organização**
  - Como parte integrante da empresa e não um “extra”
  - Possuir políticas que inclua a segurança no design dos produtos
  - Possuir políticas que incluam fornecedores, colaboradores e clientes
- **Promover atividades periódicas (ex, 1 por ano)**
  - Revisão das políticas
  - Treino e troca da experiências

Regras Importantes

Considerar a existência de dias menos bons

- **Fornecer formação aos colaboradores**
  - Para entenderem os riscos, impacto e mitigações
  - Para conhecerem as boas práticas, mecanismos e soluções
  - Que seja apoiada e aplicada em todos os níveis hierárquicos
- **Construir políticas que se apliquem a toda a organização**
  - Como parte integrante da empresa e não um “extra”
  - Possuir políticas que inclua a segurança no design dos produtos
  - Possuir políticas que incluam fornecedores, colaboradores e clientes
- **Promover atividades periódicas (ex, 1 por ano)**
  - Revisão das políticas
  - Treino e troca da experiências

Regras Importantes

Confiar mas verificar

- **Instalar os controlos adequados**
  - Tanto para atividades externas como internas
  - Sem exceções!
- **Auditorias externas são vitais**
  - Garantir que os mecanismos são efetivos
  - Garantir que as políticas cobrem os aspetos devidos
  - Garantir que as leis são observadas
- **Testes de Invasão (Pentest) são uma ferramenta importante**
  - Avaliar a existência de fraquezas na aplicação das tecnologias
  - Avaliar a existência de fraquezas nos colaboradores e processos

Regras Importantes

Partilhar Experiências, Regulamentação, Incidentes e Respostas

- **Possuir a capacidade de analisar incidentes**
  - Sobre toda a cadeia ou stack de processos e aplicações
  - Requer a existência de registos confiáveis
  - Discutir internamente, de forma alargada na empresa
- **Exercer influência externa**
  - Demonstrar como: Aplicam a regulamentação, detetam incidentes
  - Demonstrar como respondem a incidentes
  - Aumenta confiança em clientes e fornecedores