软件安全— 软件安全漏洞与防护

V1 软件缺陷与软件漏洞概述

傅建明

jmfuwhu@126.com

武汉大学国家网络安全学院

本讲提纲

- 1.1 软件缺陷与漏洞的概念
- 1.2 漏洞分类及标准
- 1.3 软件通用漏洞评估机制CVSS
- 1.4 安全事件与软件漏洞
- 1.5 软件漏洞发布平台

1.1 软件缺陷与软件漏洞

- 7·23动车事件

2011年7月23日20时30分05秒，甬温线浙江省温州市境内发生动车组列车追尾事故，造成40人死亡、172人受伤，中断行车32小时35分，直接经济损失19371.65万元。

“7·23”动车事故是由于温州南站信号设备在设计上存在严重缺陷，遭雷击发生故障后，导致本应显示为红灯的区间信号机错误显示为绿灯。

缺陷 or 漏洞？

1.1 软件缺陷与软件漏洞

1.1 软件缺陷与软件漏洞

AI 系统 Bug示例

在去年的深圳高交会上，一台名为“小胖”的机器人在没有指令的情况下突然自行打砸展台玻璃，最终导致部分展台破坏，并划伤一名观众

一名名为理查德·里（Richard Lee）的亚裔男子在试图网络更新护照的时候被新西兰内务部软件判断为“眼睛闭上，照片审核未通过”

特斯拉汽车的一场致命撞车事故，因驾驶系统不能区分白色卡车和明亮天空中出现的白云

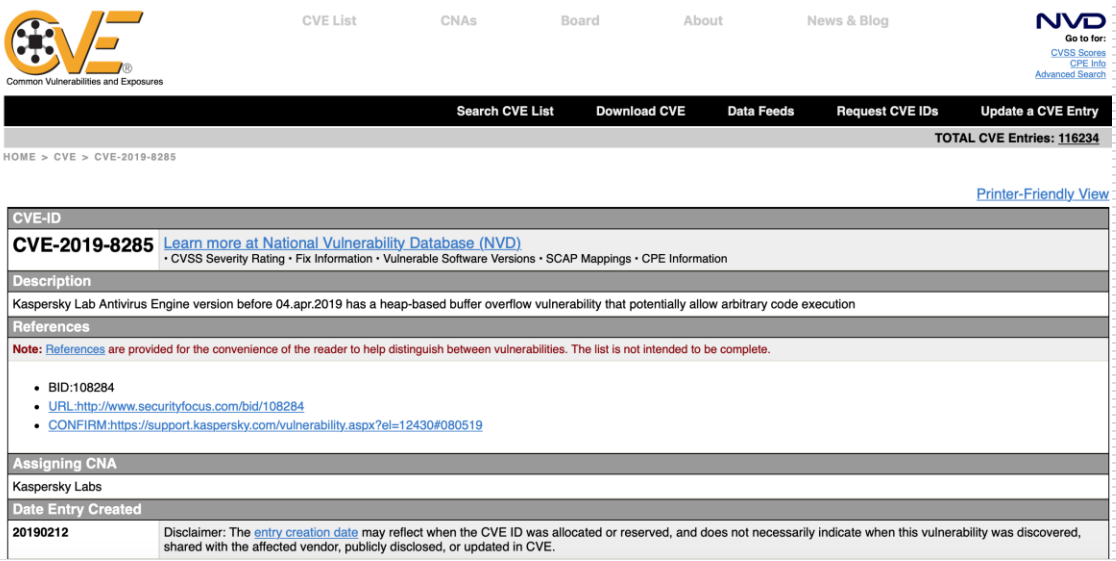
谷歌自动驾驶汽车最近爆出数起事故，例如变更车道时撞上了一辆公共汽车造成事故发生

1.1 软件缺陷与软件漏洞

- CVE-2019-8285

缺陷 or 漏洞？

由于卡巴斯基反病毒引擎其无法对用户提供的数据进行充分的边界检查，从而可能允许第三方在具有系统权限的用户PC上远程执行恶意代码。



CVE List CNAs Board About News & Blog

Common Vulnerabilities and Exposures

NVD Go to for: CVSS Scores CPE Info Advanced Search

Search CVE List | Download CVE | Data Feeds | Request CVE IDs | Update a CVE Entry

TOTAL CVE Entries: 116234

HOME > CVE > CVE-2019-8285

Printer-Friendly View

CVE-ID

CVE-2019-8285 Learn more at National Vulnerability Database (NVD)
• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Kaspersky Lab Antivirus Engine version before 04.apr.2019 has a heap-based buffer overflow vulnerability that potentially allow arbitrary code execution

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:108284
- URL:http://www.securityfocus.com/bid/108284
- CONFIRM:https://support.kaspersky.com/vulnerability.aspx?el=12430#080519

Assigning CNA

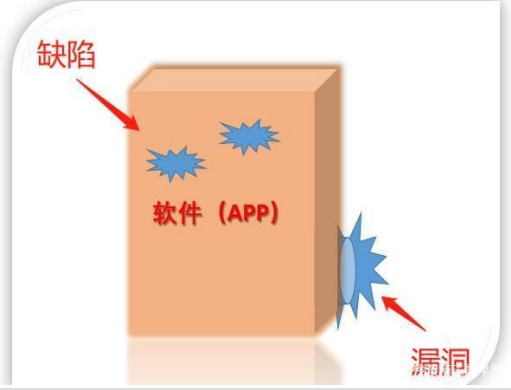
Kaspersky Labs

Date Entry Created

20190212 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.

1.1 软件缺陷与软件漏洞

- **软件缺陷：**计算机软件或程序存在某种破坏正常运行能力的问题、错误，是软件**自身固有的**。
- **软件漏洞：**软件在设计、实现、配置策略及使用过程中出现的**缺陷**，它可能导致**攻击者**利用该缺陷实现未授权访问或破坏系统。
- **基本区别：**缺陷就是软件**天然存在的**，而漏洞是被攻击者**故意利用的**缺陷。



1.1 软件缺陷与软件漏洞

软件缺陷-Bug or defect

1947年9月9日，Grace Murray Hopper在她的记录本上记下了史上第一个计算机Bug——在Harvard Mark II计算机里找到的一只飞蛾，她把飞蛾贴在日记本上，并写道”First actual case of bug being found”

“阿丽亚娜”-5运载火箭发射失败-1996年

```
char * pKeyTab;
void initKeys( int number )
{
    if (number > 0) {
     pKeyTab= \
        malloc(number*sizeof(char*));
    for (i = 0; i < number; i++)
     pKeyTab[i] = genKeyString();
    }
}
```

1.1 软件缺陷与软件漏洞

- 软件缺陷，即为计算机软件或程序中存在的某种破坏正常运行能力的问题、错误，或者隐藏的功能缺陷。(IEEE729-1983)

- **缺陷的存在会导致软件产品与用户需求不一致。**

1.1 软件缺陷与软件漏洞

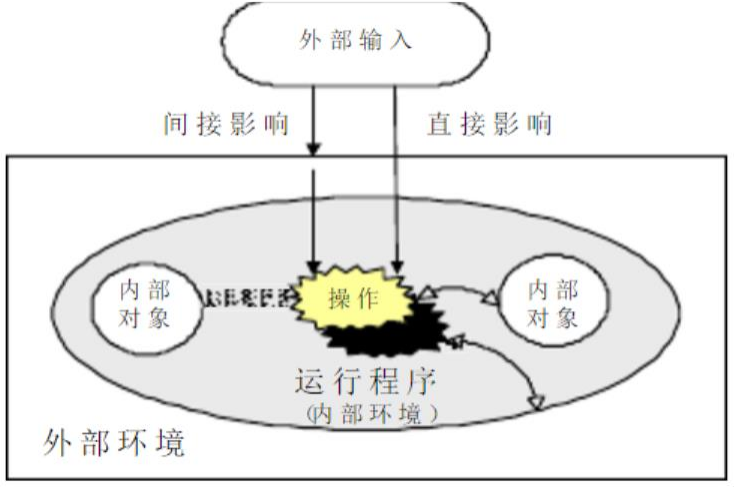
- 缺陷来源
  - Requirement
  - Architecture
  - Design
  - Code
  - Test
  - Integration
  - Environment

- 缺陷类型
  - 10 F- Function
  - 20 A- Assignment
  - 30 I- Interface
  - 40 C- Checking
  - 50 B Build/package/merge
  - 60 D- Documentation
  - 70 G- Algorithm
  - 80 U-User Interface
  - 90 P-Performance
  - 100 N-Norms

1.1 软件缺陷与软件漏洞

- 软件漏洞(Vulnerability)，通常也称脆弱性，被定义为"系统设计、实现或操作管理中存在的**缺陷或者弱点**，能被利用而**违背系统的安全策略**"(RFC2828)。

- 大多数漏洞来源
  - 逻辑错误
  - 缺陷
  - 社会工程
  - 策略失误



1.1 软件缺陷与软件漏洞

- GB/T 33561-2017归纳的漏洞成因
  - 边界条件
  - 数据验证
  - 访问验证
  - 处理逻辑
  - 同步
  - 异常处理
  - 对象验证
  - 配置
  - 设计
  - 环境


ICS 35.040
L 80

GB

中华人民共和国国家标准

GB/T 33561—2017

信息安全技术　安全漏洞分类

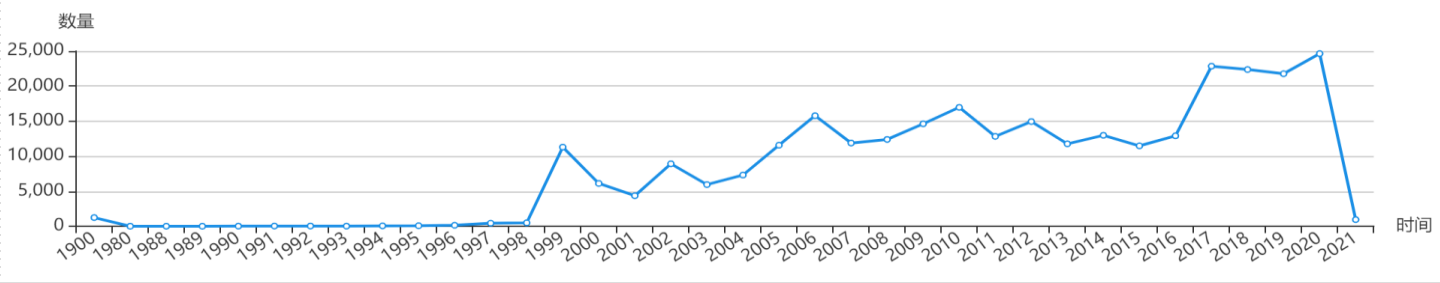
Information security technology—Vulnerabilities classification

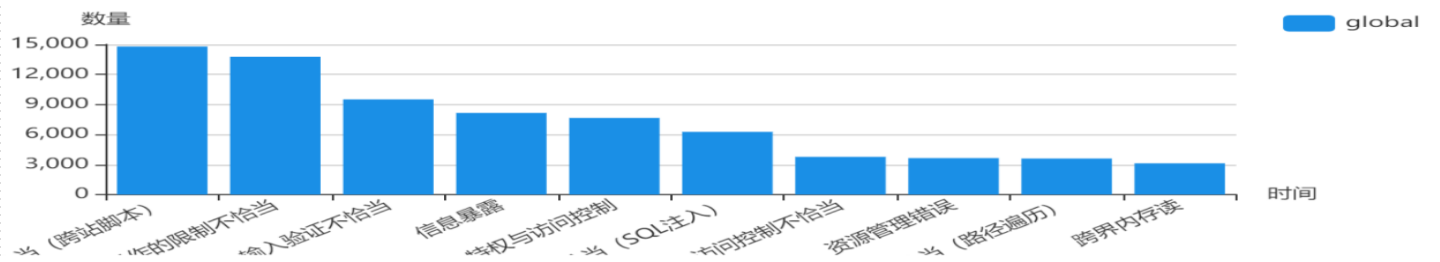
1.1 软件缺陷与软件漏洞

- 软件漏洞对系统的威胁
  - 非法获得访问权限（打印/读取/写/执行）
  - 权限提升
  - 拒绝服务
  - 恶意软件植入（主动植入/被动植入）
  - 数据丢失或者泄露（登录凭证/Password读取/Web应用的文件浏览/DNS的域传送漏洞）

1.1 软件缺陷与软件漏洞

CVE漏洞统计





1.1 软件缺陷与软件漏洞

- Web漏洞

  网站程序上的漏洞，因编写者在编写代码时考虑不周全等原因而造成的漏洞。

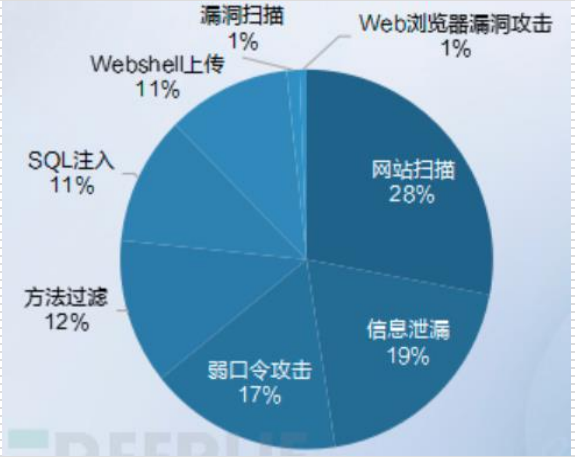
- 主要类型
  - SQL注入
  - XSS
  - 命令注入
  - CSRF
  - 目录遍历

```
select * from member where UID =' "& request("ID") &" ' And Passwd =' "& request("Pwd") & " '
select * from member where UID =' Admin '-- ' And Passwd =' '
```

```
http://.../news.aspx?id=<script>alert("XSS test");</script>
```

1.1 软件缺陷与软件漏洞

- OWASP Top Ten 2020
  - 注入（**Injection**）
  - 失效的身份认证（**Broken Authentication**）
  - 敏感数据暴露（**Sensitive Data Exposure**）
  - XML外部实体（**XXE**）
  - 失效访问控制（**Broken Access Control**）
  - 安全误配置（**Security Misconfiguration**）
  - 跨站点脚本（**XSS**）
  - 不安全的反序列化（**Insecure Deserialization**）
  - 使用具有已知漏洞的组件（**Using Components with Known Vulnerabilities**）
  - 日志记录和监视的不足（**Insufficient Logging & Monitoring**）

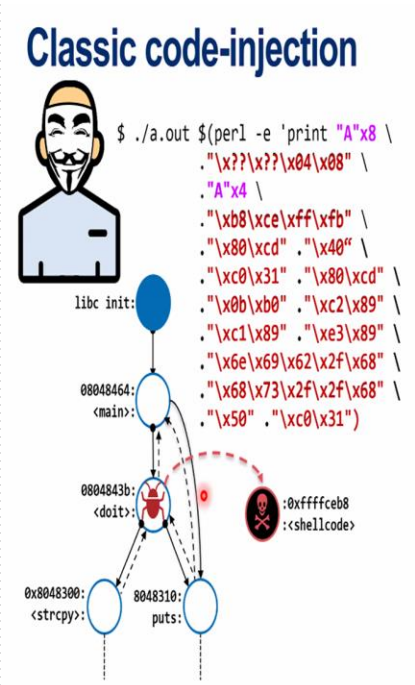


https://owasp.org/www-project-top-ten/

1.1 软件缺陷与软件漏洞

- 软件漏洞
  - 栈溢出
  - 堆溢出
  - 格式化字符串漏洞
  - 整数/浮点数溢出
  - 悬浮指针
  - 释放后引用
  - 类型混淆
  - 条件竞争
  - 逻辑漏洞

- 信息泄露
- 代码执行
  - Shellcode
  - ROP
  - PE/ELF

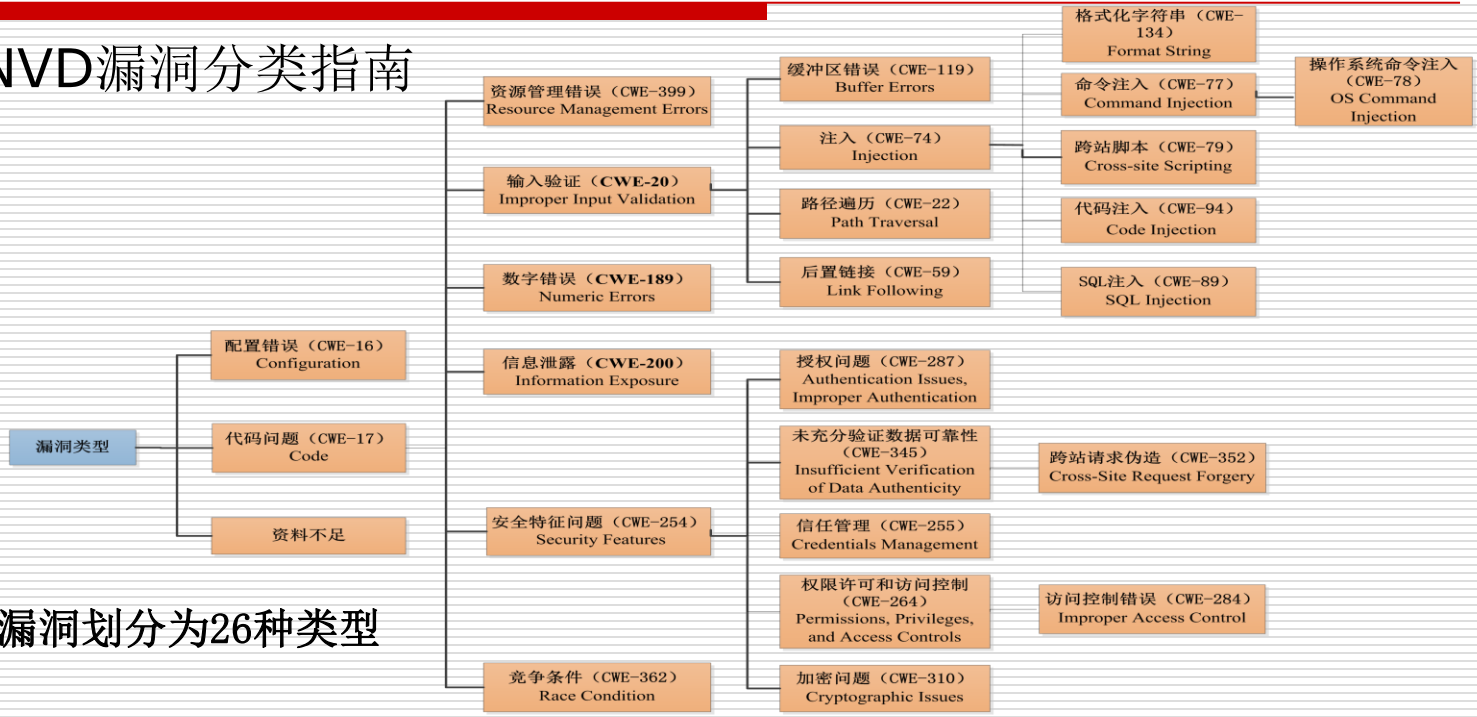


1.1 软件缺陷与软件漏洞

- 软件支持的防御
  - stackguard
  - shadow stack
  - CFG
  - CIG
  - ACG
- 系统支持的防御
  - ASLR
  - DEP or NX
- 硬件支持的防御
  - SMEP
  - SMAP
  - MPX
  - MPK
  - CET

1.2 漏洞分类及其标准

- CNNVD漏洞分类指南



信息安全漏洞划分为26种类型

http://www.cnnvd.org.cn/web/wz/bzxqById.tag?id=3&mkid=3

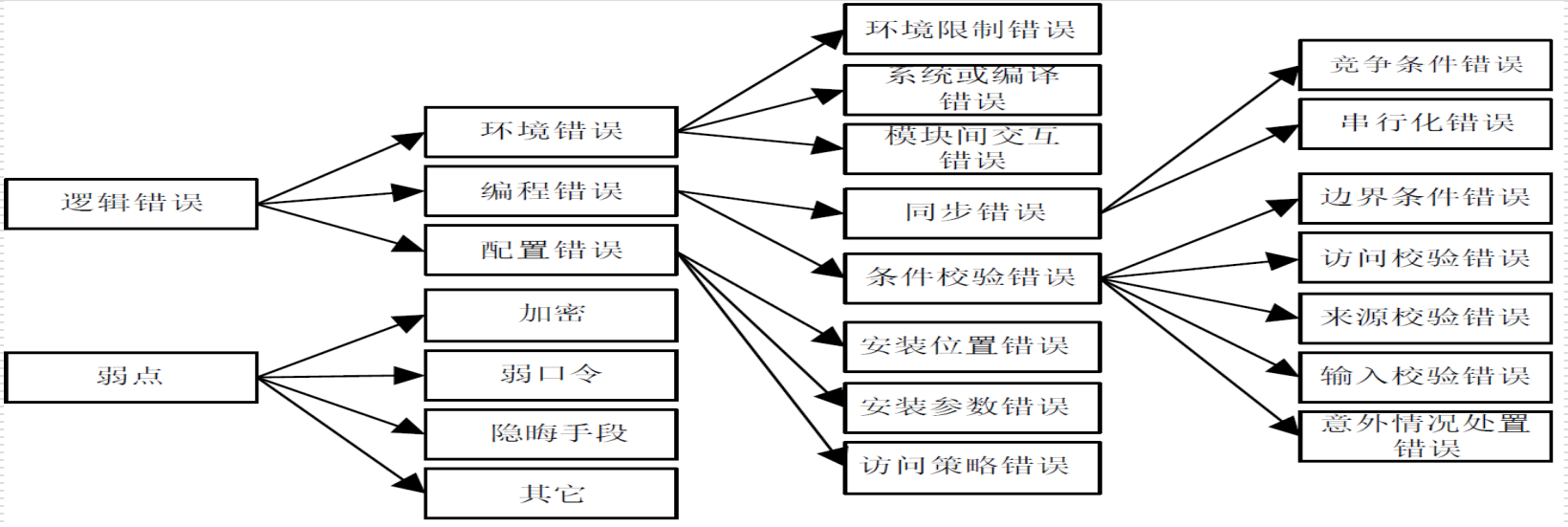
1.2 漏洞分类及其标准

- 分类原则
  - 唯一性原则：漏洞仅属于某一类别， 不存在同时属于多个类别。
  - 扩展性原则：允许根据实际情况扩展安全漏洞的类别。

- 分类依据
  - 一般可按漏洞的形成原因、所处空间和时间进行分类处理，并择一使用。

1.2 漏洞分类及其标准

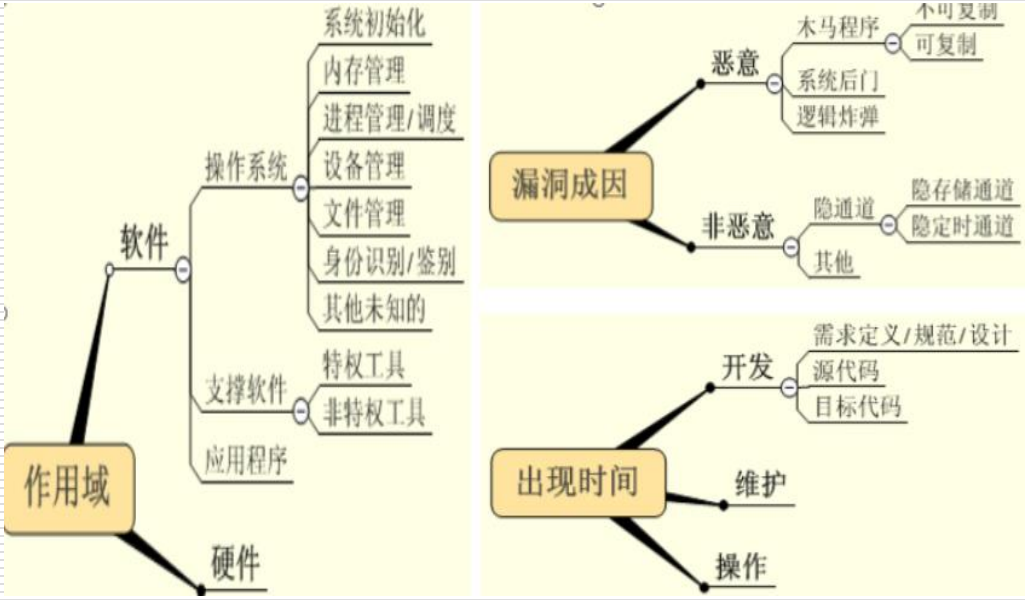
- 普渡大学的Aslam和Krsul的漏洞分类法：



Aslam T, Krsul I.Use of A Taxonomy of Security Faults.1999

1.2 漏洞分类及其标准

- Bishop的六轴分类法
  - 漏洞成因
  - 出现时间
  - 作用域
  - 利用方式
  - 漏洞利用的组件数
  - 代码缺陷



1.2 漏洞分类及其标准

- Knight的四象限
- 社会工程
  - 偷窃，钓鱼，间谍，阻挡
- 策略疏忽
  - 物理保护、数据保护、个人信息保护
- 逻辑错误
  - 应用、OS、网络、信任
- 缺陷
  - 窃听、弱口令、加密、自定义策略

- ✓ Incomplete parameter validation
- ✓ Inconsistent parameter validation
- ✓ Implicit sharing of privileged/confidential data
- ✓ Asynchronous validation/Inadequate serialization
- ✓ Inadequate identification/authentication/authorization
- ✓ Violable prohibition/limit
- ✓ Exploitable logic error

RISOS研究成果

1.2 漏洞分类及其标准

- 按照漏洞威胁
  - 获取访问权限漏洞
  - 权限提升漏洞
  - 拒绝服务漏洞
  - 恶意软件植入漏洞
  - 数据丢失或者泄露漏洞

(1) 远程管理员权限
(2) 本地管理员权限
(3) 普通用户访问权限
(4) 权限提升（沙箱）
(5) 读取受限文件
(6) 远程拒绝服务
(7) 本地拒绝服务
(8) 远程非授权文件存取
(9) 口令恢复
(10) 欺骗
(11) 服务器信息泄露

1.2 漏洞分类及其标准

- 按照漏洞成因
  - 输入验证错误。
  - 访问验证错误。
  - 竞争条件。
  - 意外情况处置错误。
  - 设计错误。
  - 配置错误。
  - 环境错误。
- 按照漏洞严重性
  - A 类漏洞（高）：威胁性最大的漏洞，往往由较差的系统管理或错误设置造成。
  - B 类漏洞（中）：较为严重的漏洞，例如允许本地用户获得增加的和未授权的访问。
  - C 类漏洞（低）：严重性不是很大的漏洞，例如允许拒绝服务的漏洞。

1.2 漏洞分类及其标准

- CWE漏洞分类
  - CWE89- SQL Injection
  - CWE78- OS Command Injection
  - CWE120-Classic Buffer Overflow
  - CWE79 - Cross-site Scripting
  - CWE306-Missing Authentication for Critical Function
  - CWE862-Missing Authorization
  - CWE798-Use of Hard-coded Credentials
  - CWE311-Missing Encryption of Sensitive Data
  - CWE434-Unrestricted Upload of File with Dangerous Type
  - CWE807-Reliance on Untrusted Inputs in a Security Decision

http://cwe.mitre.org/top25/index.html

1.2 漏洞分类及其标准

- 微软的漏洞严重性分级
  - **Critical**

    RCE
  - **Important**

    RCE with user action, Information Disclosure
  - **Moderate**

    DOS with sys, Information Disclosure with given location
  - **Low**

    DOS with app, non-sensitive Information Disclosure

https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2A3xt

1.2 漏洞分类及其标准

- Pure-FTPd 缓冲区错误漏洞
  - 发布时间：2020-02-24
  - CVE编号：CVE-2020-9365
  - CNNVD编号：CNNVD-202002-1111
  - 危害级别：高危
  - 威胁类型：远程
  - 漏洞类型：缓冲区错误
  - 漏洞来源：Gentoo
  - 漏洞详情：Pure-FTPd 1.0.49版本中的utils.c文件的‘pure_strcmp’函数存在缓冲区错误漏洞。远程攻击者可借助特制请求利用该漏洞导致拒绝服务。

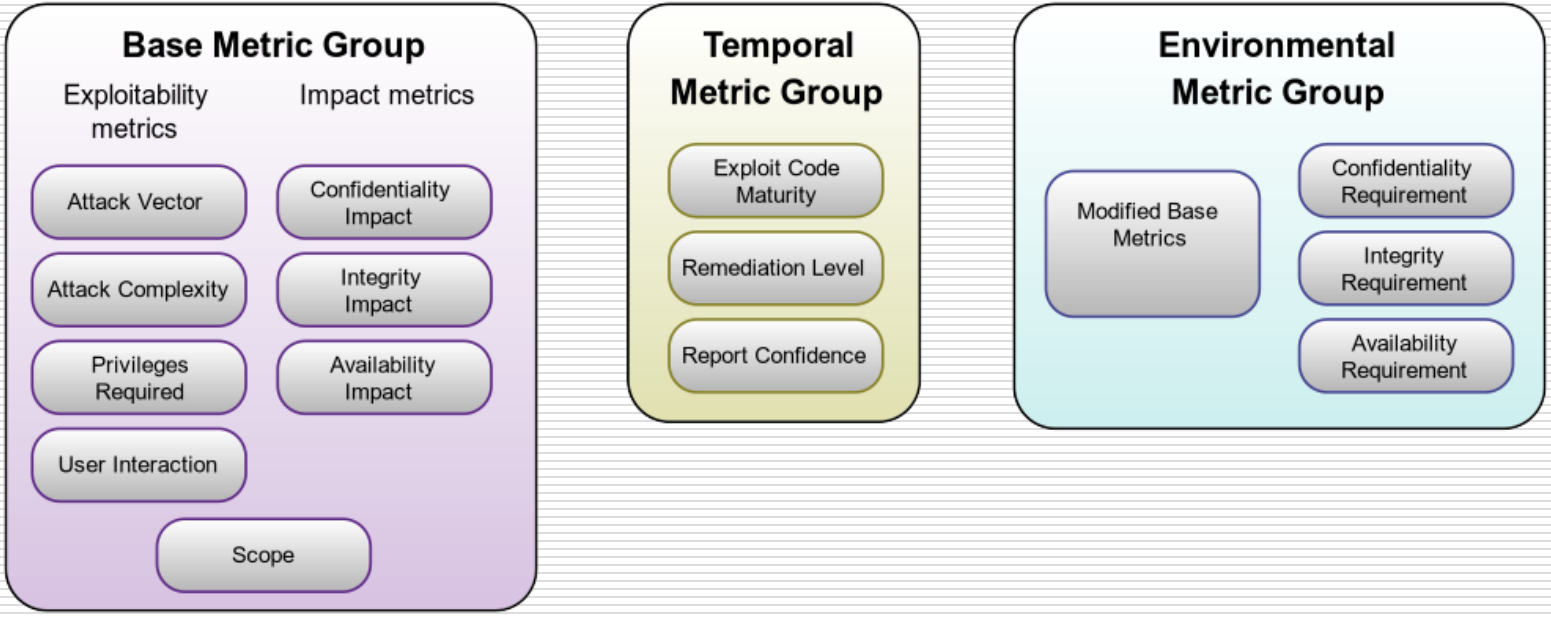
```
int pure_strcmp(const char * const s1, const char * const s2)
{
-   return pure_memcmp(s1, s2, strlen(s1) + 1U);
+   const size_t s1_len = strlen(s1);
+   const size_t s2_len = strlen(s2);
+   if (s1_len != s2_len) {    return -1;    }
+   return pure_memcmp(s1, s2, s1_len);
}
```

1.3 漏洞评估机制CVSS

- CVSS-Common Vulnerability Scoring System
- 度量指标
  - **基础 – Base**
    描述漏洞的固有特性
  - **时间 – Temporal**
    描述漏洞随时间而改变的特性
  - **环境 – Environmental**
    描述漏洞与特殊用户环境相关的特性

https://www.first.org/cvss/

1.3 漏洞评估机制CVSS



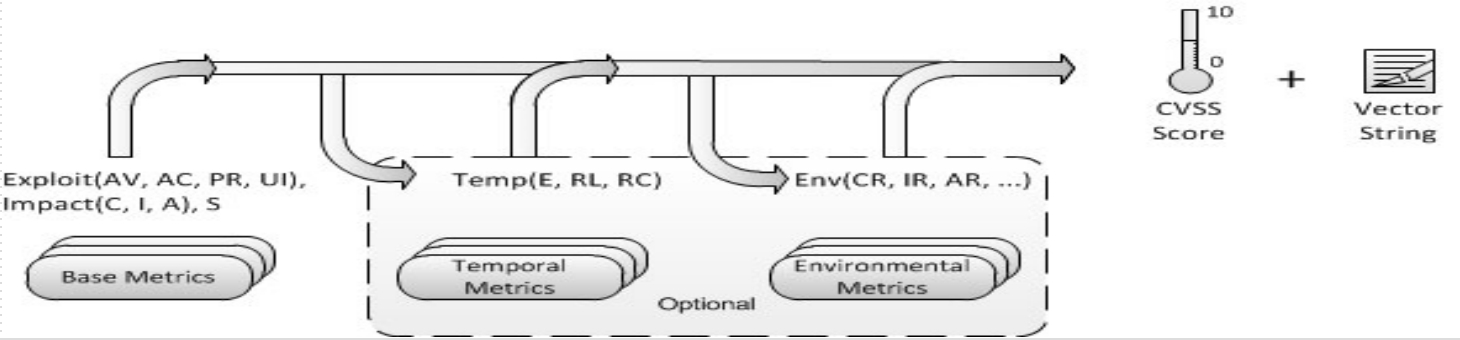
1.3 漏洞评估机制CVSS

基础分数（必须）	
可利用性指标(Exploitability Metrics)	
攻击向量(AV)	网络(N) 相邻(A) 本地(L) 物理(P)
攻击的复杂性(AC)	低(L) 高(H)
所需的特权(PR)	没有(N) 低(L) 高(H)
用户交互(UI)	没有(N) 要求(R)
范围(Scope)	
范围(S)	不变(U) 改变(C)
影响指标(Impact Metrics)	
机密性(C)	没有(N) 低(L) 高(H)
完整性(I)	没有(N) 低(L) 高(H)
可用性(A)	没有(N) 低(L) 高(H)

1.3 漏洞评估机制CVSS

时间分数（可选）	
利用代码的成熟度(E)	未定义(X) 未经验证(U) PoC(P) 函数(F) 高(H)
修复级别(RL)	未定义(X) 官方修复(O) 临时修复(T) 工作区(W) 不可用(U)
报告的可信度(RC)	未定义(X) 未知(U) 合理(R) 确认(C)
环境分数（可选）	
机密性要求(CR)	未定义(X) 低(L) 中(M) 高(H)
完整性要求(IR)	未定义(X) 低(L) 中(M) 高(H)
可用性要求(AR)	未定义(X) 低(L) 中(M) 高(H)
修改基础度量指标 (Modified Base Metrics)	Modified Attack Vector (MAV) Modified Attack Complexity (MAC) Modified Privileges Required (MPR) Modified User Interaction (MUI) Modified Scope (MS)/Modified Confidentiality (MC) Modified Integrity (MI)/Modified Availability (MA)

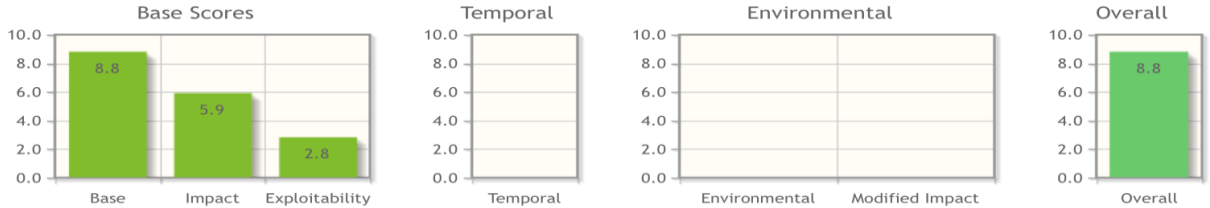
1.3 漏洞评估机制CVSS



RATING	CVSS SCORE
None	0.0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	**9.0 – 10.0**

Common Vulnerability Scoring System Calculator Version 3 CVE-2019-8285

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

Show Equations

CVSS v3 Equations

The CVSS v3.0 equations are defined below.

Base

The Base Score is a function of the Impact and Exploitability sub score equations. Where the Base score is defined as,

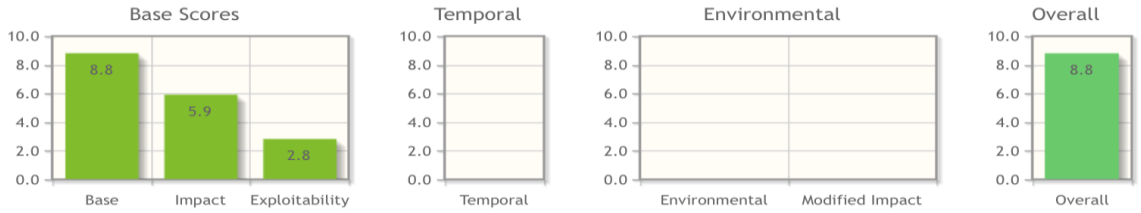
$$\begin{array}{ll} \textit{If (Impact sub score <= 0)} & \textit{0 else,} \\ \textit{Scope Unchanged}_4 & \textit{Roundup}(\textit{Minimum}[(\textit{Impact} + \textit{Exploitability}), 10]) \\ \textit{Scope Changed} & \textit{Roundup}(\textit{Minimum}[1.08 \times (\textit{Impact} + \textit{Exploitability}), 10]) \end{array}$$

and the Impact sub score (ISC) is defined as,

$$\begin{array}{l} \textit{Scope Unchanged}\ 6.42 \times \textit{ISC}_{\text{Base}} \\ \textit{Scope Changed}\ 7.52 \times [\textit{ISC}_{\textit{Base}} - 0.029] - 3.25 \times [\textit{ISC}_{\textit{Base}} - 0.02]^{15} \end{array}$$

Common Vulnerability Scoring System Calculator Version 3 CVE-2019-8285

This page shows the components of the CVSS score for example and allows you to refine the CVSS base score. Please read the CVSS standards guide to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



CVSS Base Score: 8.8
Impact Subscore: 5.9
Exploitability Subscore: 2.8
CVSS Temporal Score: NA
CVSS Environmental Score: NA
Modified Impact Subscore: NA
Overall CVSS Score: 8.8

Show Equations

CVSS v3 Vector
AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H

3.Base Merics具体计算方法

3.1 Exploitability可执行性块

攻击向量（AV）	网络（N）/邻居（A）/本地（L）/物理（P）	0.85 / 0.62 / 0.55 / 0.2
攻击复杂度（AC）	低（L）/高（H）	0.77 / 0.44
权限要求（PR）	无（N）/低（L）/高（H）	0.85 / 0.62(0.68) / 0.27(0.50)
用户交互（UI）	不需要（N）/需要（R）	0.85 / 0.62
影响范围（UI）	不改变（U）/改变（C）	根据*Impact sub score和ISC取值*

3.2 Impact影响指标

机密性（C）	无（N）/低（L）/高（H）	0 / 0.22 / 0.56
完整性（I）	无（N）/低（L）/高（H）	0 / 0.22 / 0.56
可用性（A）	无（N）/低（L）/高（H）	0 / 0.22 / 0.56

4.Time具体计算方法

利用代码的成熟度（E）	未验证（U）/PoC（P）/EXP（F）/自动化利用（H）	0.91 / 0.94 / 0.97 / 1
修复方案（RL）	正式补丁（O）/临时补丁（T）/缓解措施（W）/不可用（U）	0.95 / 0.96 / 0.97 / 1
来源可信度（RC）	未知（U）/未完全确认（R）/已确认（C）	0.92 / 0.96 / 1

5.Environmental具体计算方法

环境分数（可选）	
机密性要求(CR)	未定义(X) 低(L) 中(M) 高(H)
完整性要求(IR)	未定义(X) 低(L) 中(M) 高(H)
可用性要求(AR)	未定义(X) 低(L) 中(M) 高(H)
修改基础度量指标 (Modified Base Metrics)	Modified Attack Vector (MAV) Modified Attack Complexity (MAC) Modified Privileges Required (MPR) Modified User Interaction (MUI) Modified Scope (MS) Modified Confidentiality (MC) Modified Integrity (MI) Modified Availability (MA)

1.4 安全事件与软件漏洞

- 软件漏洞分析方向：

  1）从具体的安全事件出发，探究安全事件的要素，以及要素的关联。

  - 乌克兰电网攻击安全事件
  - 其他的典型网络安全事件

  2）从具体的软件漏洞出发，探究漏洞的机理。

  - 沙虫漏洞
  - 其他软件漏洞

1.4 安全事件与软件漏洞

- 乌克兰电网攻击安全事件：

  2015年12月23日，乌克兰电力部门遭受到**恶意代码攻击**，乌克兰新闻媒体TSN在24日报道称：“至少有三个电力区域被攻击，并于当地时间15时左右导致了**数小时的停电事故**”；“攻击者**入侵了监控管理系统**，超过一半的地区和部分伊万诺-弗兰科夫斯克地区断电几个小时。

- 安全事件的要素：
  - 攻击时间
  - 攻击对象
  - 攻击手段（恶意代码）
  - 攻击后果

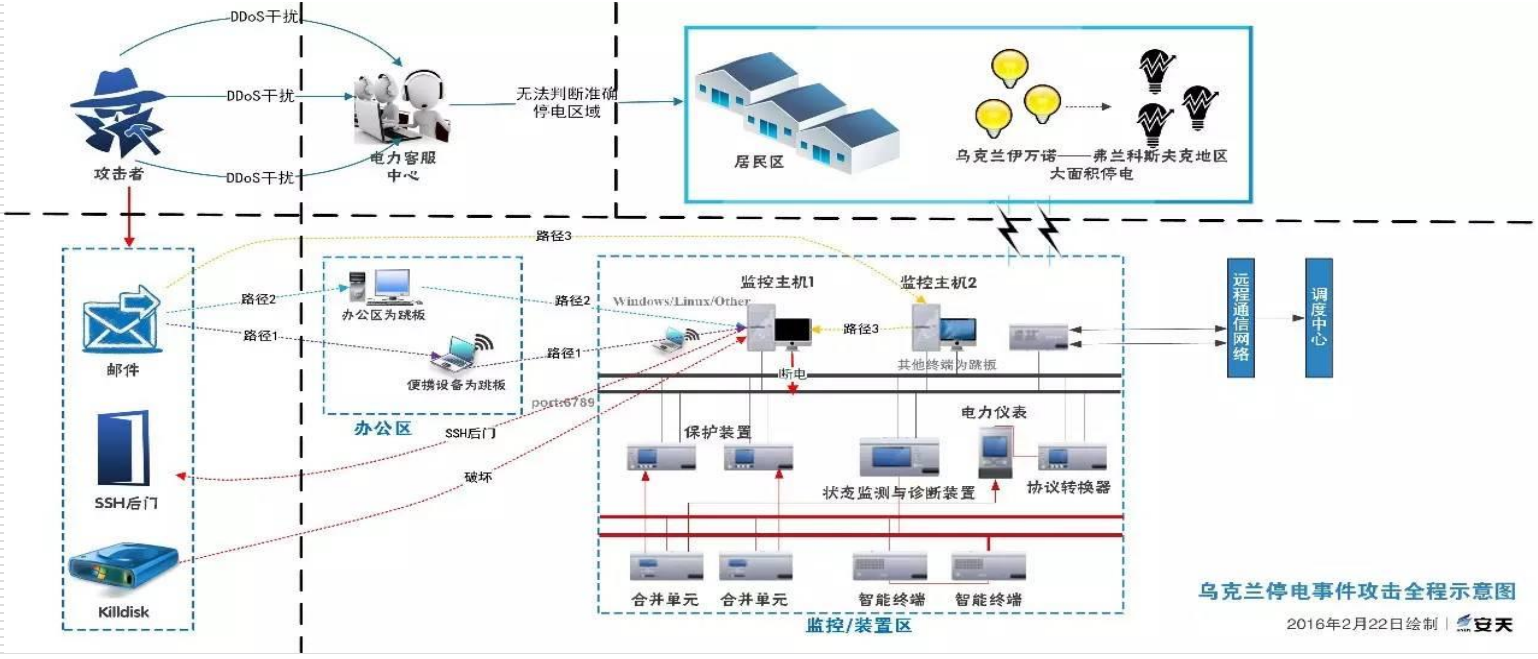
1.4 安全事件与软件漏洞

- 技术性描述：

  安全公司ESET在2016年1月3日表示乌克兰电力部门感染的是恶意代码**BlackEnergy**，BlackEnergy被当作后门使用，并释放了**KillDisk**破坏数据来延缓系统的恢复。同时在其他服务器还发现一个添加后门的**SSH程序**，攻击者可以根据内置密码随时连入受感染主机。BlackEnergy曾经在2014年被黑客团队**"SandWorm"**用于攻击欧美SCADA工控系统。"沙虫"使用了Windows OLE远程代码执行漏洞**(CVE-2014-4114)**。

- 安全事件的要素：+ 软件漏洞

1.4 安全事件与软件漏洞



1.4 安全事件与软件漏洞

□ （网络）安全事件：

攻击者在给定的时间段内，利用漏洞或者其他攻击手段[在攻击对象中注入并触发恶意代码]，产生拒绝服务、信息泄露、信息窃取、目标控制等后果的过程。

2020

- ✓ 雅诗兰黛泄露4.4亿数据记录
- ✓ 迪卡侬1.23亿个人信息泄露（Decathlon）
- ✓ 暴露超过1.35亿的客户个人记录（SOS云备份）
- ✓ 委内瑞拉国家电网干线遭攻击，全国大面积停电
- ✓ 本田汽车遭勒索软件重创
- ✓ 新西兰证交所连续一周遭受DDoS攻击导致交易中断
- ✓ 微软Bing应用数据库多达1亿条搜索纪录被泄露
- ✓ 美国1.86亿选民数据在暗网被黑客出售

2020

- ✓ 富士康被黑客攻击，索要2.3亿赎金
- ✓ 巴西卫生部官网泄露2.43亿巴西人个人信息
- ✓ 某行的顾客信息泄露
- ✓ solarwinds供应链事件

1.4 安全事件与软件漏洞

- CVE2014-4114

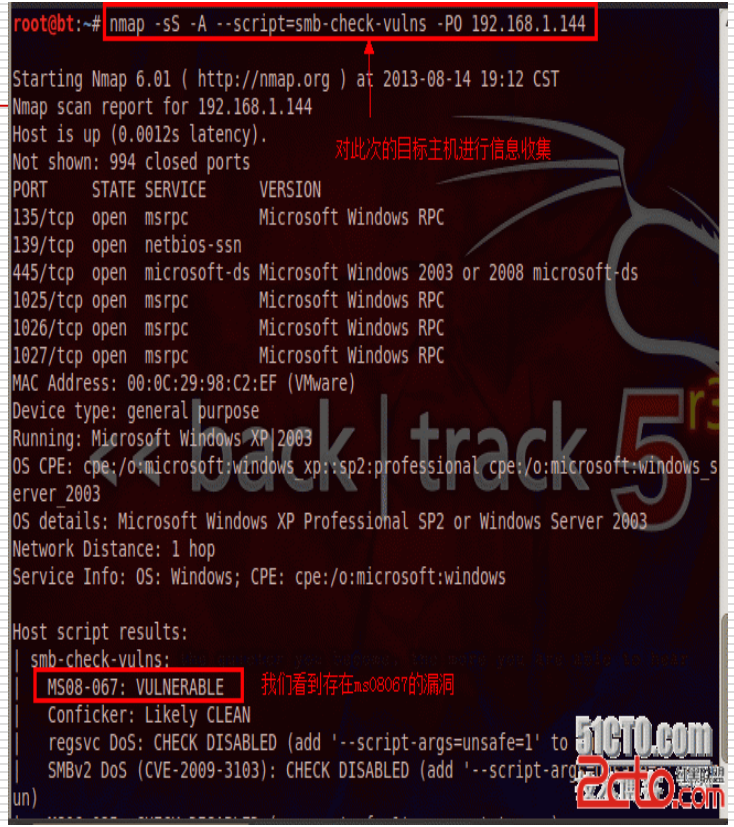
  Microsoft Windows OLE中存在一个漏洞，如果用户打开包含特制OLE对象的文件，则该漏洞可能允许远程执行代码。成功利用此漏洞的攻击者可以获得与登录用户相同的用户权限。如果当前用户使用管理用户权限登录，则攻击者可随后安装程序；查看、更改或删除数据；或者创建拥有完全用户权限的新帐户。那些帐户被配置为拥有较少用户权限的用户比具有管理用户权限的用户受到的影响要小。

- 影响版本

  Windows Vista SP2，Windows Server 2008 SP2，Windows 7 SP1，Windows Server 2008 R2 SP1，Windows 8，Windows 8.1，Windows Server 2012，Windows Server 2012 R2，Windows RT 和 Windows RT 8.1

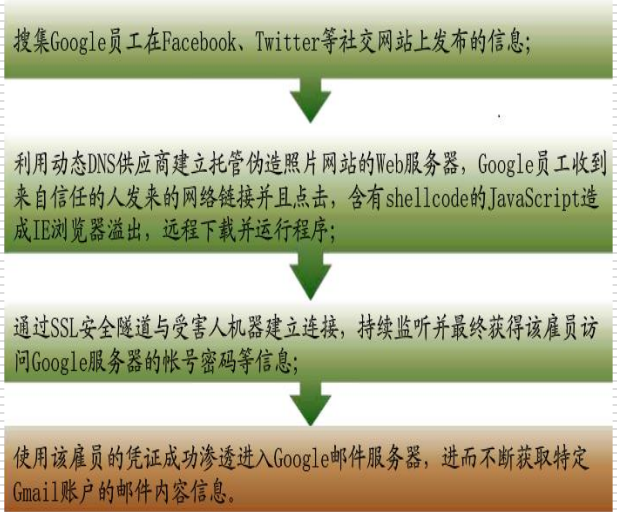
蠕虫王和飞客

- 2003年1月—蠕虫王，存在于内存中拒绝服务-（CVE2002-1123，缓冲区溢出）
- 2008年11月-飞客，远程控制、信息获取-（MS08-067，RPC缓冲区溢出）



极光行动

- 2009年12月中旬的“极光行动”(Aurora)-**IE漏洞(MS10-002/018)**, 攻击的企业有Google、Adobe Systems、Juniper Networks、Rackspace、雅虎、赛门铁克、诺斯洛普·格鲁门、陶氏化工等20多家企业
- 控袭Gmail服务器

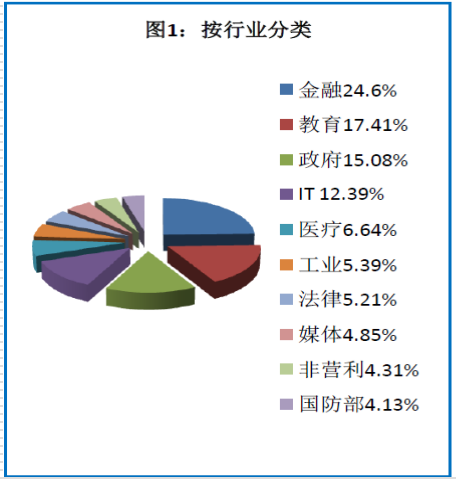


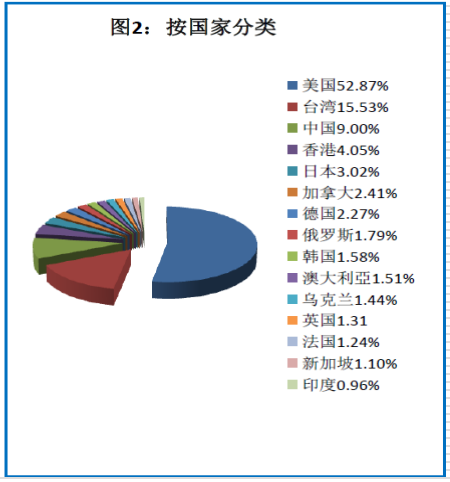
暗鼠行动

- 2011年8月份,McAfee和Symantec公司发现并报告了暗鼠行动（ Operation Shady RAT)。该攻击从2006年启动,在长达数年的持续攻击过程中,控制全球多达72个公司和组织的网络,包括美国政府、联合国、红十字会、武器制造商、能源公司、 金融公司等等。

隐秘山猫

- 2013年2月， BIT9披露了该公司客户遭受的攻击（“隐秘山猫”，Hidden Lynx）
- 商业间谍和政府承包商





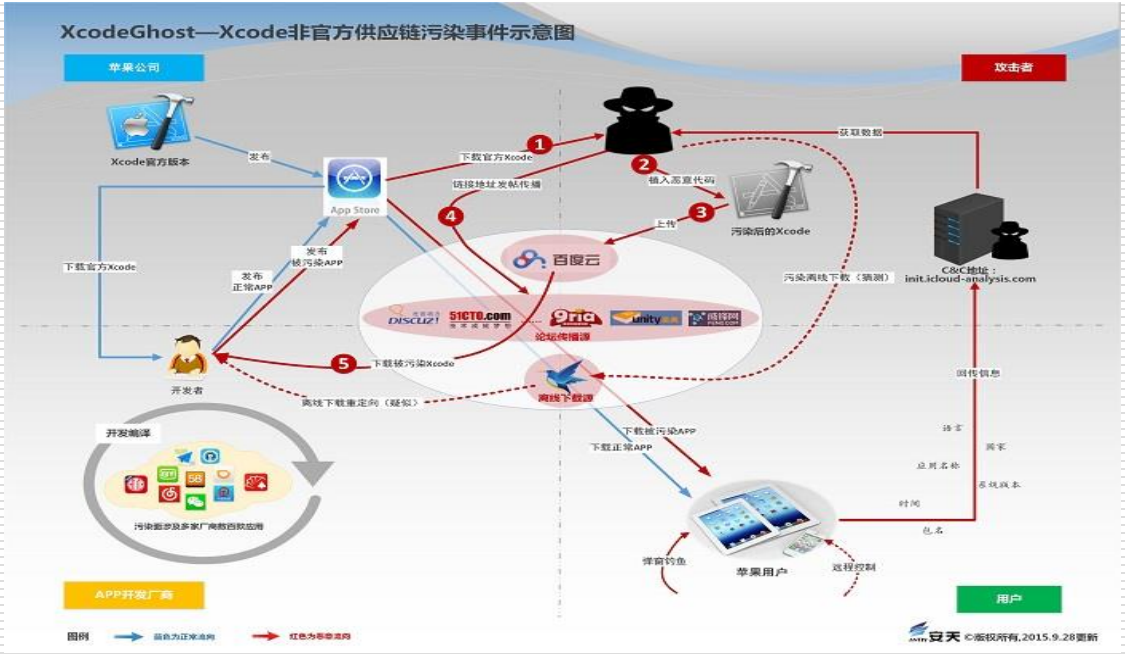
XCodeGhost

- Ken Thompson，1983年图灵奖获得者
  - UNIX，C语言
- Ken Thompson（肯·汤普森）在编译器中植入后门
  - Pattern2是编译器，如果发现正在编译器，则把后门代码添加到可执行文件中

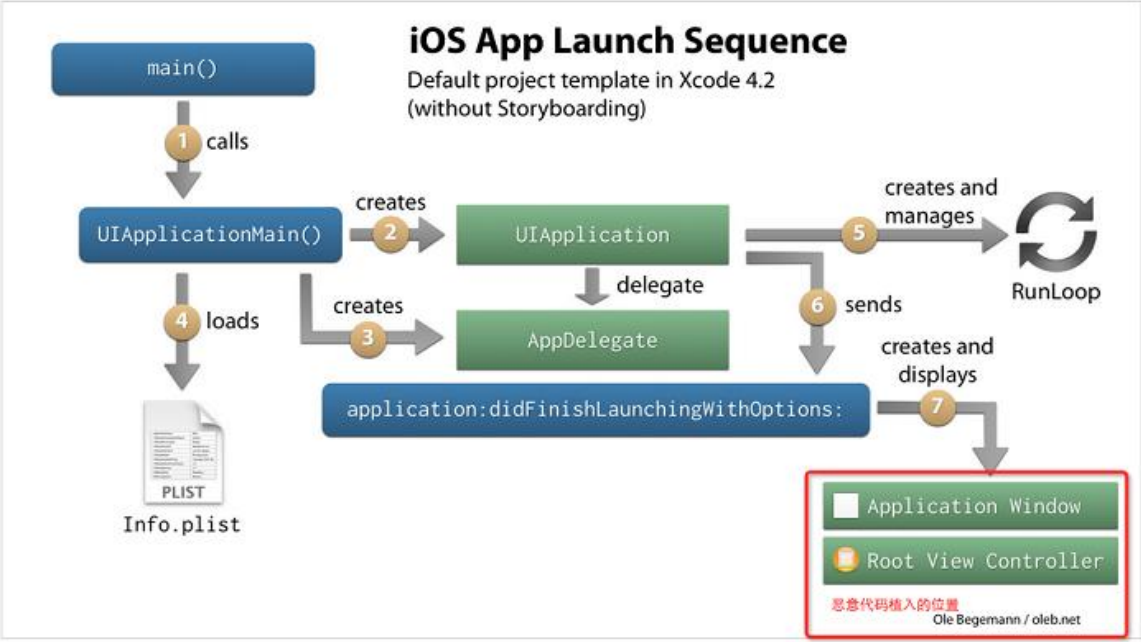
```
compile(s)
char *s;
{
        if(match(s, "pattern1")) {
                compile ("bug1");
                return;
        }
        if(match(s, "pattern 2")) {
                compile ("bug 2");
                return;
        }
        ...
}
```

Thompson K. Reflections on trusting trust[J]. Communications of the ACM, 1984, 27(8): 761-763.

XCodeGhost

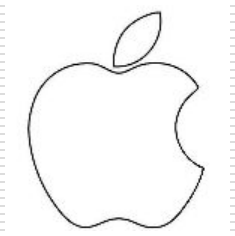

XcodeGhost—Xcode非官方供应链污染事件示意图
苹果公司
攻击者
Xcode官方版本
发布
App Store
下载官方Xcode
链接地址发帖传播
植入恶意代码
上传
污染后的Xcode
获取数据
C&C地址：
init.icloud-analysis.com
污染离线下载（猜测）
百度云
论坛传播源
离线下载源
下载官方Xcode
发布
正常APP
发布
被污染APP
开发者
下载被污染Xcode
离线下载重定向（疑似）
开发调试
污染覆盖及多家厂商数百款应用
下载被污染APP
下载正常APP
回传信息
语言
国家
应用名称
系统版本
时间
包名
弹窗钓鱼
苹果用户
远程控制
APP开发厂商
用户
图例
蓝色为正常流向
红色为恶意流向
©版权所有,2015.9.28更新

XCodeGhost


iOS App Launch Sequence
Default project template in Xcode 4.2
(without Storyboarding)
main()
1 calls
UIApplicationMain()
creates
2
UIApplication
creates and manages
5
RunLoop
delegate
4 loads
creates
3
AppDelegate
6 sends
creates and displays
7
application:didFinishLaunchingWithOptions:
PLIST
Info.plist
Application Window
Root View Controller
恶意代码植入的位置
Ole Begemann / oleb.net

XCodeGhost

- APP的恶意功能
- 上传隐私：时间戳、应用名、包名、系统版本、语言、国家、网络信息等
- 远控模块：OpenURL（URL scheme ）远控
  - 调用App
  - 拨打电话
  - 发送短信
  - 发送邮件
  - 获取剪贴板信息
  - 打开网页，如打开高仿Apple的钓鱼网站
  - 结合弹窗推广应用（社工：取消->安装）
- 中间人利用：利用域名劫持感染的设备



XCodeGhost

- 结果：感染1078款APP
- 溯源：
  - 开发者没有从原厂下载Xcode
  - 开发者没有验证下载工具的合法性
  - 开发者没有严格测试开发的App
  - 国家没有严格的监控手段

TOP 200排行
1 微信
2 百度
3 淘宝
4 QQ
5 高德导航
6 搜狗输入法
7 百度视频
8 滴滴打车
9 爱奇艺PPS影音
10 网易新闻
……

21 我叫MTOnline
22 优酷视频
……
52 铃声大全
53 百度音乐
54 美团团购
……
59 查违章
60 爱奇艺视频
61 限时免费大全
……
101 芒果TV
102 网易云音乐
103 今日头条
……
200 冰川时代：村庄

http://bobao.360.cn/news/detail/2088.html

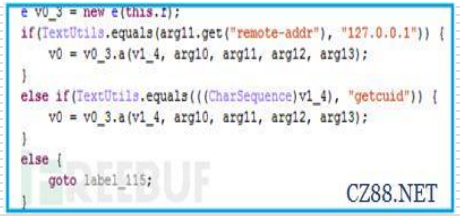
Wormhole

- 2015年10月28日，乌云漏洞平台曝百度旗下多款App存在WormHole漏洞。

- 已知受影响的App包括：百度地图、百度浏览器、百度贴吧、百度翻译、百度视频、百度手机助手、百度云、百度音乐、百度新闻、百度图片、百度输入法等。（4,014 种）
  - 应用安装到手机上之后，它会打开40310/6259端口，任何IP都可以连接该端口。
  - immortal service（不朽端口）：一个监听40310/6259端口的app被卸载，另一个app会 立马启动服务重新监听40310/6259端口

Wormhole

- 百度的Moplus SDK存在一个后门，该后门简单验证了Http头部的remote-addr
  - 获取手机信息
  - 扫描下载文件
  - 给手机增加联系人
  - 下载任意文件
  - 上传任意文件
  - APK静默安装



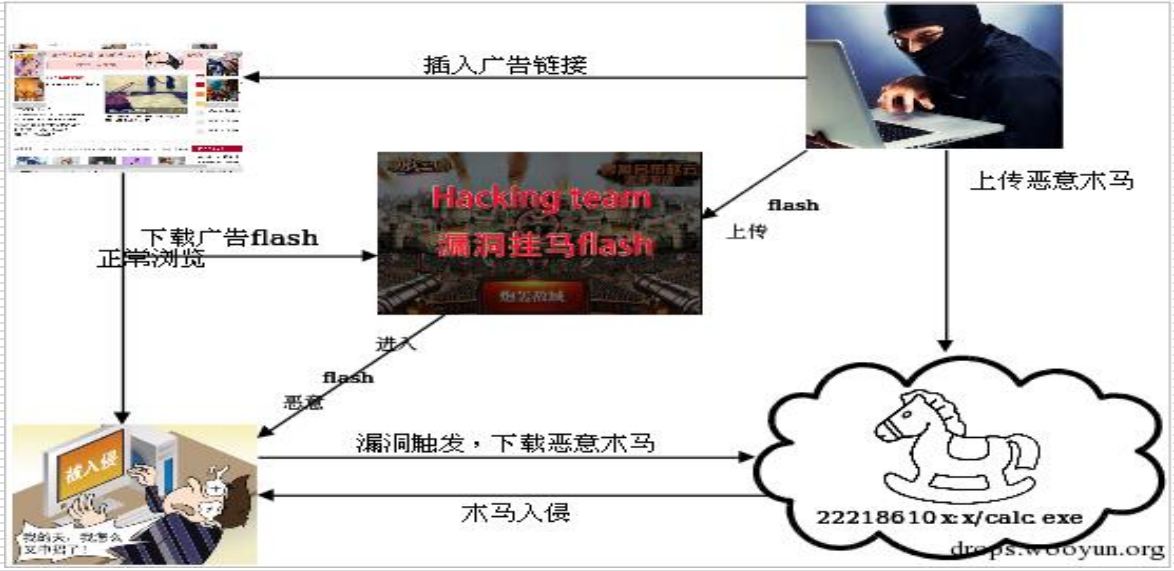
Hacking Team

- Hacking Team
  - 意大利的软件开发商
  - 出售漏洞、攻击工具、攻击平台

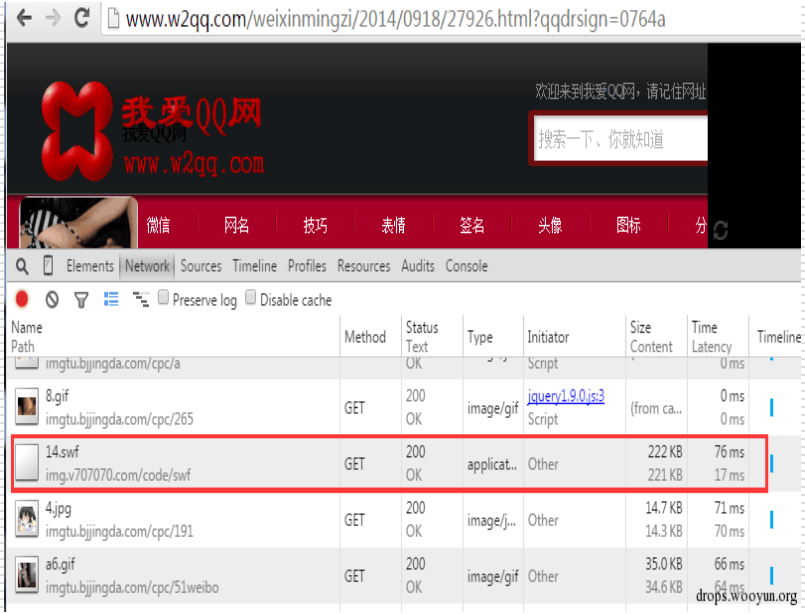
- 2015年7月5日，Hacking Team遭遇了大型数据攻击泄漏事件
  - Flash player、Windows字体、Word、PPT、Excel、Android的未公开漏洞、IE、Chrome（打开文档、浏览网页中马）
  - 全平台的木马后门程序 （监控微信、whatsapp、skype ）

Hacking Team

- 入侵过程：网页植入广告、触发Flash漏洞、下载木马



Hacking Team



1.5 漏洞发布平台

- CVE-Common Vulnerabilities Exposures
  - http://cve.scap.org.cn （中文）
  - http://cve.mitre.org
- 美国国家信息安全漏洞库
  - http://nvd.nist.gov
- 中国国家信息安全漏洞库
  - http://www.cnnvd.org.cn

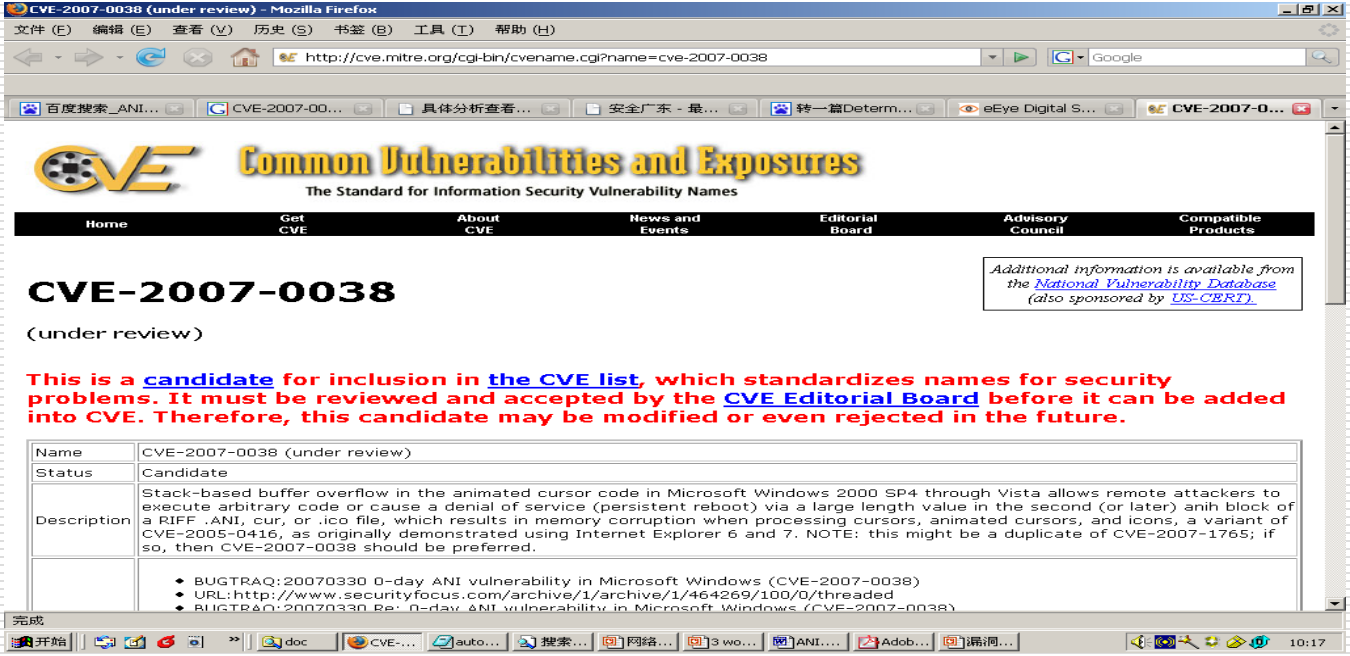
1.5 漏洞发布平台

- https://www.seebug.org/（知道创宇）
- https://www.butian.net/(360)
- https://www.microsoft.com/zh-cn/msrc?rtc=1
- https://source.android.com/security/bulletin/
- SecurityFocus
- Redhat Bugzilla
- ExploitDB
- OpenWall
- SecurityTracker

1.5 漏洞发布平台

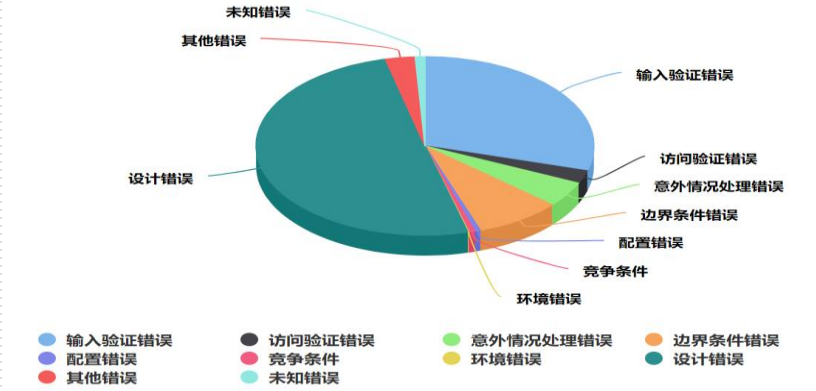
- MiTRE公司于1999年建立了"通用漏洞列表"（Common Vulnerability and Exposures,CVE）
  - 为每个漏洞和暴露确定了唯一的名称
  - 给每个漏洞和暴露一个标准化的描述
  - 不是一个数据库，而是一个字典
  - 任何完全迥异的漏洞库都可以用同一个语言表述
  - 由于语言统一，可以使得安全事件报告更好地被理解，实现更好的协同工作
  - 可以成为评价相应工具和数据库的基准
  - 非常容易从互联网查询和下载
  - 通过“CVE编辑部”体现业界的认可

1.5 漏洞发布平台


CVE-2007-0038 (under review) - Mozilla Firefox
http://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2007-0038
Common Vulnerabilities and Exposures
The Standard for Information Security Vulnerability Names
Home
Get CVE
About CVE
News and Events
Editorial Board
Advisory Council
Compatible Products
CVE-2007-0038
(under review)
Additional information is available from the National Vulnerability Database (also sponsored by US-CERT).
This is a candidate for inclusion in the CVE list, which standardizes names for security problems. It must be reviewed and accepted by the CVE Editorial Board before it can be added into CVE. Therefore, this candidate may be modified or even rejected in the future.
Name
CVE-2007-0038 (under review)
Status
Candidate
Description
Stack-based buffer overflow in the animated cursor code in Microsoft Windows 2000 SP4 through Vista allows remote attackers to execute arbitrary code or cause a denial of service (persistent reboot) via a large length value in the second (or later) anih block of a RIFF .ANI, cur, or .ico file, which results in memory corruption when processing cursors, animated cursors, and icons, a variant of CVE-2005-0416, as originally demonstrated using Internet Explorer 6 and 7. NOTE: this might be a duplicate of CVE-2007-1765; if so, then CVE-2007-0038 should be preferred.
BUGTRAQ:20070330 0-day ANI vulnerability in Microsoft Windows (CVE-2007-0038)
URL:http://www.securityfocus.com/archive/1/archive/1/464269/100/0/threaded

1.5 漏洞发布平台

- 国家信息安全漏洞共享平台（Chinese National Vul Database）http://www.cnvd.org.cn/
  - 基础电信运营商
  - 网络安全公司
  - 软件厂商
  - 互联网企业
  - 国家重点企业



1.5 漏洞发布平台

http://www.cnvd.org.cn/

课后思考

- 以最近一则安全新闻为例，剖析其安全事件的本质及背后的技术机理。
- 讨论人（用户）在网络安全事件的作用。
- 有人说“漏洞的原因是程序代码存在条件语句”，如何理解该结论？
- 因人和环境而产生的漏洞有哪些？
- 如何防御和检测漏洞攻击？