Vulnerability handling
DK-CERT

TF-CSIRT, Heraklion, 21. May 2010

Shehzad Ahmad, DK-CERT
Email: shehzad.ahmad@uni-c.dk
Agenda

- Introduction of DK-CERT
  - Background, today and the future

- DK-CERT Services

- Vulnerability Handling
  - Vulnerability database
    - Our own database

- Scanning report
  - How is the scanning done?
  - How is the result presented in the report
Who is DK-CERT?

- DK-CERT is an organization of UNI•C, Danish IT Center for Education and Research - an agency under the Ministry of Education.

- UNI•C created DK-CERT in 1991 in connection with one of the first hacker cases in Denmark.


- Our main task is to work as an Academic CERT.
DK-CERT and GovCERT

Have agreed to deliver “National CERT” services.

- Services for the citizens
  - Security information, alerts, vulnerabilities -> on website borger.dk
  - Mailing list -> allows us to send out information directly to the citizens
  - 1881 (public free number for citizens) IT-security calls in office hours
  - FAQ (approx 100 questions/answers)
  - (will be using facebook and twitter as well)

- Services for SME
  - Security information, alerts, vulnerabilities, on website virk.dk
  - Mailing list for companies

- Continue working with the ISP’s
- Media, Police and other important partners…
DK-CERT activities -> Incident Handling.

- DK-CERT receives reports of security incidents (Incident Handling), from outside and from the networks we monitor: Danish network for Research and Education (Forskningsnettet), and the network of UNI•C.

- 2006: 55.000
- 2007: 90.000
- 2008: 46.000
- 2009: 37.000

- (Standard incident reports as: phishing sites, port-scans, hacking incidents, spam etc.)
Type of cases handled by DK-CERT

<table>
<thead>
<tr>
<th>Type</th>
<th>2008</th>
<th>2009</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phishing</td>
<td>279</td>
<td>446</td>
</tr>
<tr>
<td>Denial of Service</td>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>Hacking</td>
<td>331</td>
<td>1217</td>
</tr>
<tr>
<td>Portscan</td>
<td>44666</td>
<td>33761</td>
</tr>
<tr>
<td>Root compromise</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>Spam</td>
<td>84</td>
<td>178</td>
</tr>
<tr>
<td>Trojan</td>
<td>42</td>
<td>105</td>
</tr>
<tr>
<td>Virus</td>
<td>5</td>
<td>15</td>
</tr>
<tr>
<td>Warez (copyright)</td>
<td>580</td>
<td>1649</td>
</tr>
</tbody>
</table>

Port scan
DK-CERT services

- Security scans
  - Normal vulnerability (port & service) scan
  - Deep application (WEB-servers, SQL-databases) scan
  - Wireless network scan (routers, encryption status, configuration etc. (coming up)

- Vulnerability database.
  - Mainly for Danish network for Research and Education (Forskningsnettet)

- Reverse engineering on malware (on hold at the moment).

- Awareness campaigns
  - Weekly newsletters, columns, articles, interviews etc….
  - We use Facebook (since 2008) and we are “testing” Twitter
  - Trend report 2009 (available in danish and english) (and new Q1 2010 report)
<table>
<thead>
<tr>
<th>Reactive Services</th>
<th>Proactive Services</th>
<th>Security Quality Management Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>+ Alerts and Warnings</td>
<td>+ Announcements</td>
<td>✓ Risk Analysis</td>
</tr>
<tr>
<td>+ Incident Handling</td>
<td>+ Technology Watch</td>
<td>✓ Business Continuity &amp; Disaster Recovery Planning</td>
</tr>
<tr>
<td>- Incident analysis</td>
<td>+ Security Audit or Assessments</td>
<td>✓ Security Consulting</td>
</tr>
<tr>
<td>- Incident response on site</td>
<td>+ Configuration &amp; Maintenance of Security Tools, Applications, &amp; Infrastructures</td>
<td>✓ Awareness Building</td>
</tr>
<tr>
<td>- Incident response support</td>
<td>+ Development of Security Tools</td>
<td>✓ Education/Training</td>
</tr>
<tr>
<td>- Incident response coordination</td>
<td>+ Intrusion Detection Services</td>
<td>✓ Product Evaluation or Certification</td>
</tr>
<tr>
<td>+ Vulnerability Handling</td>
<td>+ Security-Related Information Dissemination</td>
<td></td>
</tr>
<tr>
<td>- Vulnerability analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Vulnerability response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Vulnerability response coordination</td>
<td></td>
<td></td>
</tr>
<tr>
<td>+ Artifact Handling</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Artifact analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Artifact response</td>
<td></td>
<td></td>
</tr>
<tr>
<td>- Artifact response coordination</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
DK-CERT’s Vulnerability database
How will the customer use the Vulnerability database?

• The customer chooses what applications and operating systems, he/she will receive alerts on.

• Vulnerability database collects warnings and information on vulnerabilities from the Internet

• Customer receives regular lists of updates to the applications and systems he/she has chosen.
How are warnings received by the user?

Warnings can be received in different ways:
- E-mail
- SMS*
- DK-CERT’s website
- RSS-feed - customer made*
- Customers own site
From where are the vulnerability information received?

- nvd.nist.gov
- OS-vendors – ex. Microsoft, Debian, Red Hat, Ubuntu, HP-UX
- The system can be extended - we can retrieve information from all those who publish vulnerabilities in a fairly fixed format.
Vulnerability database

Customer

Vulnerability Service (database)

List of applications and systems
Specific warnings about vulnerabilities

Warning

Microsoft

UNIX, Linux, other OS

NIST, other public sources
Vulnerability

- One unique CVE id
- Short description
- Solution
- Vulnerable systems
- References (vendor-specific advisories)
- Possibility for specific vendor-related descriptions and features
- Different searchable dates
- CVSS-score, extendible

**Short description**
Use-after-free vulnerability in Apple Safari 4.0.5 on Windows allows remote attackers to execute arbitrary code by using `window.open` to create a popup window for a crafted HTML document, and then calling the parent window's `close` method, which triggers improper handling of a deleted window object.

**Solution**
For further details about a solution look under references.

**Vulnerable systems:**
See list
apple safari 4.0.5

**Advisory references and solutions**
- Advisory from CERT-VN (Original advisory)
- Advisory from VUPEN (Original advisory)
- Advisory from BID (Original advisory)
- Advisory from OSVDB (Original advisory)
- Advisory from SECTRACK (Original advisory)
- Advisory from SECUHIA (Original advisory)
- Advisory from MISC (Original advisory)
- Advisory from MISC (Original advisory)

**Source**
NIST
Advisory

- Description
- Solution
- References to vulnerabilities
- Possibility for vendor-specific descriptions, solutions, and features

2010-05-02 squidguard -- buffer overflow
Source: DEBIAN
ID: DSA-2040

Description
It was discovered that in squidguard, a URL redirector/filter/ACL plugin for squid, several problems in src/sqLog.c and src/sqDiv.c allow remote users to either:

- cause a denial of service, by requesting long URLs containing many slashes; this forces the daemon into emergency mode, where it does not process requests anymore.
- bypass rules by requesting URLs whose length is close to predefined buffer limits, in this case 2048 for squidguard and 4096 or 8192 for squid (depending on its version).

Solution
For the stable distribution (lenny), this problem has been fixed in version 1.2.0-3.4+lenny1.
For the unstable distribution (sid), this problem has been fixed in version 1.2.0-9.
We recommend that you upgrade your squidguard package.

Advisory from vendor
Advisory from DEBIAN
http://www.debian.org/security/2010/dsa-2040

Vulnerabilities
The following vulnerabilities affect this advisory

- CVE-2009-2709
  Failure to Constrain Operations within the Bounds of a Memory Buffer
- CVE-2009-3826
  Failure to Constrain Operations within the Bounds of a Memory Buffer
System

- Containers with name
- OS, application or hardware name with version
- Wildcards including not yet existing versions
- Systems can contain systems
Vulnerabilities

1. NIST
2. Vendor sites
3. Web interface

DK-CERT's VDB

Advisories and systems

Vulnerabilities and systems
Future work

- Improve CVSS usage
- Use CPE (Common Product Enumeration) more
- More use of containers
- Integration with vulnerability scannings
- Improve registering of systems
- Better visualisation of systems, vulnerabilities and advisories
  - Statistics of vulnerabilities and advisories
  - Better overview of registered systems, vulnerabilities and advisories
DK-CERT’s
Scanning and reporting system
Vulnerability scanning

Who are we scanning?

- Organizations connected to the Danish Research Network (Forskningsnettet).
- Other organizations on request.

What are we scanning?

- Public IP-address spaces.
- TCP Ports 0-1024 and ports listed in nmap’s list of well-known ports and ICMP.

Why are we scanning?

- To prevent compromise of data and systems in the scanned organizations.
- To assist the administrators in securing their systems.
- To assist in rendering visibility of risk management.
- As a part of revision - and occasionally as part of analysis of compromised systems.
Vulnerability scanning

The scanning process:

1. Port detection with Nmap.

2a. OS- and service detection with Nmap.

2b. Vulnerability scanning with Nessus.

2c. Vulnerability scanning with OpenVAS.

3. Application scanning on http/https services with Nikto.


Customer reports.
Vulnerability scanning

a) **initiate port scanning** from costume made web application.

b) automated initiation of **vulnerability scanning's** with costume made scripts.

c) automated initiation of **web application scanning's** with costume made scripts.

d) automated **export of results** to costume made web application.

e) **generation of report** in costume made web application.
Vulnerability scanning

System overview

Costumer database (CRM):
- costumer information
- network information
- system information

Vulnerability database (webapp):
- vulnerability information
- CVSS information
- system information

Scanning management application:
- management (who, when, what)
- analyzes
- comments
- reports
- statistics

Scannings applications:
- Nmap
- Nessus
- OpenVas
- Nikto

Customer reports.

User validation
- user information
- costumer information
- network information
- system information

Customer & network information

Scannings information (what)

Scannings results
Vulnerability scanning

Reports are:

- generated from the scanning management application.
- costume made.
- the result of both the results, analysis, manual and automated tests.

The costume made reports:

- are in html format with pdf pages for print.
- has functionality for managing the patch management process.
- includes parts for both, management, it-security and it administrators.
Vulnerability scanning

The report
- How does it look?
Vulnerability scanning

The report (easy navigation):

- overviews sorted on ip-adresses, ports & vulnerabilities.
- print management
- management of responsibilities and updates.
Vulnerability scanning

Presentation of the results for the customer with the report.

- The report is presented remotely to the costumer(s) on an Adobe Connect installation on Danish Research Network.

- The costumer can download the report from Adobe Connect.

- As a control for the security responsible, the costumer can get a rescan.
[ Thank you for listening !]
[Questions?]

Shehzad Ahmad
Email: shehzad.ahmad@uni-c.dk
DK-CERT