Vulnerability database
DK-CERT

TF-CSIRT September 2010
Istanbul

Morten Bartvig, DK-CERT
Email: morten.bartvig@uni-c.dk
Agenda

- Introduction of DK-CERT
- DK-CERT Services
- Vulnerability database
Who is DK-CERT?

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

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

- **Awareness campaigns**
  - Weekly newsletters, columns, articles, interviews etc….
  - Trend report 2009 (available in danish and english)
DK-CERT’s Vulnerability database
Vulnerability database

Customer

List of applications and systems

Vulnerability Service (database)

Specific warnings about vulnerabilities

Microsoft

UNIX, Linux, other OS

NIST, other public sources

Warning

Warning

Warning
Vulnerabilities

- NIST
- Vendor sites
- CERT's VDB
- Web interface

1. Vulnerabilities And systems
2. Advisories and systems
3. Vulnerabilities And systems
# Vulnerability

- One unique CVE id
- Short description
- Vulnerable systems
- References (vendor-specific advisories)
- Different searchable dates
- CVSS-score, extendible

## Modified date
2010-05-14

## Publication date
2010-05-13

## CVE
CVE-2010-1939

## CVSS-score
![High CVSS-score](image)

More details on CVSS-score

## 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
<table>
<thead>
<tr>
<th>Advisory from CERT-VN</th>
<th>Original advisory</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advisory from VUPEN</td>
<td>Original advisory</td>
</tr>
<tr>
<td>Advisory from BID</td>
<td>Original advisory</td>
</tr>
<tr>
<td>Advisory from OSVDB</td>
<td>Original advisory</td>
</tr>
<tr>
<td>Advisory from SECTRACK</td>
<td>Original advisory</td>
</tr>
<tr>
<td>Advisory from SECUNIA</td>
<td>Original advisory</td>
</tr>
<tr>
<td>Advisory from MISC</td>
<td>Original advisory</td>
</tr>
<tr>
<td>Advisory from MISC</td>
<td>Original advisory</td>
</tr>
</tbody>
</table>

## Source
NIST
Advisories via webmonitor

Vendor sites

Advisories And systems

CERT's VDB

Vendors
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/msgLog.c and src/msgDiv.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 1.2.0-8.4+lenny.
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-2009-3700: 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
Parsers

Internet → Parsers
- Debian
- Redhat
- BID
- Microsoft
- ...

→ VDB
Parser

### Regexes

```
(?>\t+\s*\t*)(?!CVE-\d+-\d+)
(Microsoft\s(?:\w+\s)+ ... )
<div id="vulnerability">\s+
<span class="title">([^<>]+)<\/span>```

### Custom code

```php
<?php
class DEBIAN extends CustomRegex {
    function DEBIAN () {
        // systems
        if (preg_match_all ('/\<h3\>Debian GNU/Linux ...')
    }
}
```
Backend vs. frontend

MVC framework (CakePHP)
- Who is vulnerable?
- Advice customers
- Get newest CPE
- Make statistics
- Return advisories and vulnerabilities

PHP/HTML, CMS, other application
- Show vulnerabilities and advisories
- Make containers
- Register systems
- Show statistics

XML-RPC

Web

Ajax
MVC framework

- **Controller**: Receives input and decides actions
- **Model**: Domain-specific representation of data
- **View**: XML, HTML
Common European VDB

Collaboration

More parsers

More specialized features

Common platform

Happier and safer end users
Central VDB

**Downsides**
- Serve many clients
- SPOF
- Slow "chain of command"

**Upsides**
- Only local frontends
Decentralized VDB

**Downsides**
- Different software versions

**Upsides**
- No central server maintenance
- Customized backends
Common VDB

- Default frontend and backend
- Customizable frontend and backend
- Other apps can collect data from VDB (vuln scan)
- Make calls to external applications
- Plugins to LDAP servers, etc.
- Extended CVSS features
- Possibly CWE support
- Possibly update CPE names
- Enhanced features for sorting and organizing
- Decentralized experimentation with new features
Advantages in DK-CERT's Vuln db

- Easily extendible parsing system
- Conversion from a specific vendor's naming conventions to standard CPE names
- Flexible extendible system for registering OS, applications and hardware
- Flexible container system
- Ability for end user to choose between vulnerabilities and advisories
[ Thank you for listening !]
[Questions?]

Morten Bartvig
Email: morten.bartvig@uni-c.dk
DK-CERT