0-Day Patch
Exposing vendors (in)security performance

BlackHat Europe 2008 – Amsterdam

Stefan Frei + Bernhard Tellenbach
Communication Systems Group
ETH Zurich – Switzerland
http://www.csg.ethz.ch
http://www.techzoom.net/risk
Evolution of the Security Ecosystem

- What is the performance of software vendors?
- How many patches available at 0-Day?
- Does responsible disclosure really work?
- Global trends vs. vendor specific issues
What is a 0-Day Patch?

- Lifecycle of a vulnerability - exposure time

Non-0-Day Patch

0-Day Patch

min. window of exposure: 0-days
What is the Disclosure-Date?

Our requirements:

- Vulnerability information is freely available to public
- Disclosed by a trusted and independent source
- Vulnerability is analyzed and rated by experts

Disclosure-Date of a vulnerability:

Date of the first advisory issued by a trusted and independent source
## Data Sources

<table>
<thead>
<tr>
<th>Source</th>
<th>Unique CVEs</th>
<th>Advisories</th>
<th>DiscoDat</th>
<th>ExploDat</th>
<th>DisclDat</th>
<th>PatchDat</th>
</tr>
</thead>
<tbody>
<tr>
<td>microsoft.com</td>
<td>992</td>
<td>611</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>611</td>
</tr>
<tr>
<td>frsirt.com</td>
<td>10771</td>
<td>10120</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10120</td>
</tr>
<tr>
<td>iss.net</td>
<td>27595</td>
<td>36483</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>32048</td>
</tr>
<tr>
<td>secunia.com</td>
<td>16246</td>
<td>21131</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>21131</td>
</tr>
<tr>
<td>secwatch.org</td>
<td>5238</td>
<td>13940</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>10903</td>
</tr>
<tr>
<td>securitytracker.com</td>
<td>8233</td>
<td>12083</td>
<td>0</td>
<td>6075</td>
<td>12082</td>
<td>0</td>
</tr>
<tr>
<td>apple.com</td>
<td>820</td>
<td>101</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>101</td>
</tr>
<tr>
<td>oracle.com</td>
<td>335</td>
<td>33</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>33</td>
</tr>
<tr>
<td>nvd.gov</td>
<td>28464</td>
<td>28464</td>
<td>0</td>
<td>0</td>
<td>28357</td>
<td>0</td>
</tr>
<tr>
<td>cert.org</td>
<td>2246</td>
<td>2380</td>
<td>5</td>
<td>0</td>
<td>2377</td>
<td>0</td>
</tr>
<tr>
<td>securityfocus.com</td>
<td>21573</td>
<td>24789</td>
<td>0</td>
<td>0</td>
<td>24698</td>
<td>0</td>
</tr>
<tr>
<td>mitre.org</td>
<td>26053</td>
<td>29797</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>zerodayinitiative.com</td>
<td>120</td>
<td>136</td>
<td>136</td>
<td>0</td>
<td>136</td>
<td>0</td>
</tr>
<tr>
<td>defense.com</td>
<td>570</td>
<td>567</td>
<td>509</td>
<td>7</td>
<td>559</td>
<td>0</td>
</tr>
<tr>
<td>milw0rm.com</td>
<td>1872</td>
<td>2279</td>
<td>0</td>
<td>2056</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>redhat.com</td>
<td>1678</td>
<td>1160</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1139</td>
</tr>
<tr>
<td>osvdb.org</td>
<td>24996</td>
<td>38908</td>
<td>3487</td>
<td>13482</td>
<td>38416</td>
<td>0</td>
</tr>
<tr>
<td>mozilla.org</td>
<td>238</td>
<td>186</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>126</td>
</tr>
<tr>
<td>adobe.com</td>
<td>65</td>
<td>132</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>132</td>
</tr>
</tbody>
</table>
0-Day patch: Overall performance

Interpretation of plots

- 0-Day patch rate since 2002
- For High and Medium risk vulnerabilities patched till Dec 2007
- Sliding window, 360 days
- Green (0-day patch) measures share of the responsible disclosure process
- Blue+Red measure the performance of vendor to produce a patch in 30 or 90 days
- Grey, do we ever get a patch? (ever = in less than 180 days)

Y-Axis:
Fraction of vulnerabilities patched in less than:

- 1 day (0-day)
- 30 days
- 90 days
- 180 days after disclosure

X-Axis:
time (years)

# Vulnerabilities patched between 2002-2008
Apple: 738
Microsoft: 658
0-Day Patch: Microsoft

- 0-Day patch rate between 40-80%, huge variation within 5 years
- Correlation with development of new OS or service pack (next slide)
0-Day Patch: Microsoft

WinXP SP1 (2002-09-09)
WinSrv 2003 (2003-04-24)
WinXP SP2 (2004-08-06)
WinSrv 2003 SP1 (2005-03-30)
WinSrv 2003 R2 (2005-12-05)
WinSrv 2003 SP2 (2007-03-13)
Win Vista (2007-01-30)

http://www.techzoom.net/risk – BlackHat 2008 Europe
# of Unpatched Vulnerabilities: Microsoft

Y-Axis:
Number of unpatched vulnerabilities

X-Axis:
time (years)

- Evolution of the number of unpatched vulnerabilities at a certain date
## 0-Day Patch: Apple

- 0-Day patch rate between 0-70%, slow start
- Coordinated disclosure took-off no earlier than end 2003
0-Day Patch: Apple

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
<th>Date Released</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS X 10.2 Jaguar</td>
<td>(2002-08-02)</td>
<td></td>
</tr>
<tr>
<td>OS X 10.3 Panther</td>
<td>(2003-10-24)</td>
<td></td>
</tr>
<tr>
<td>OS X 10.4 Tiger</td>
<td>(2005-04-29)</td>
<td></td>
</tr>
<tr>
<td>iPhone</td>
<td>(2007-06-29)</td>
<td></td>
</tr>
<tr>
<td>OS X 10.5 Leopard</td>
<td>(2007-10-26)</td>
<td></td>
</tr>
</tbody>
</table>

APPLE, 738 high+medium patches, 2002-01-01 to 2008-01-01
# Unpatched Vulnerabilities: Apple

Y-Axis: Number of unpatched vulnerabilities

X-Axis: time (years)

- OSX 10.3 “Panther” (October 23, 2003)
- OSX 10.4 “Tiger” (April 29, 2005) delayed due to i-Phone
- OSX 10.5 “Leopard” (October 26, 2007)
- i-Phone release (USA) (June 29, 2007)

Evolution of the number of unpatched vulnerabilities at a certain date
High- and Medium Risk Patches: Apple vs. Microsoft

Y-Axis:
Fraction of vulnerabilities patched in less than:
- **1 day (0-day)**
- **30 days**
- **90 days**
- **180 days**

X-Axis:
Time (years)

# Vulnerabilities
- **Apple**: 738
- **Microsoft**: 658
#Unpatched Vulnerabilities: Apple vs. Microsoft

**Apple**

- **Y-Axis:** Number of unpatched vulnerabilities
- **X-Axis:** time (years)

**Microsoft**

- **# Unpatched Vulnerabilities** (Average)
- **Apple:** increasing
- **Microsoft:** stable
What does this mean?

- **High and medium risk**
  - Coordinated disclosure process is either at a high level (MS) or has increased considerably (Apple)
  - Fraction of vulnerabilities with 0-day patch is both surprisingly high and shockingly low over last 5 years
  - Service pack and OS development binds (security) resources

- **Number of concurrent unpatched vulnerabilities**
  - Microsoft: Remains in the same range (impacted by software lifecycle > devel. resources)
  - Apple: trend shows increasing number (to few resources to cope with side-effects of increased popularity of their products?)
Conclusion

- Introduction of 0-day patch as viable metric to measure the security processes of vendors
- Metric based on publicly available data
- First analysis of the 0-day (in)security performance of software vendors at this scale
- “Unbiased” data set by correlating information from multiple sources to antagonize possible bias in vendor information

Future

- Continued monitoring and database updates
- Implications and applications of these findings to security ecosystem and risk analysis models
Thank you

- All plots are online at http://www.techzoom.net/risk
- Feedback and comments highly appreciated

Research sponsored by

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Swiss Federal Institute of Technology, Zurich
www.csg.ethz.ch