Prudent Patching

Bob McCoy, CISSP/ISSAP, MCSE
Technical Account Manager
Premier Support
Microsoft Corporation

Definition

pru·dent (prōōd'nt) adj.

1. Wise in handling practical matters; exercising good judgment or common sense.

2. Careful in regard to one's own interests; provident.

3. Careful about one's conduct; circumspect.
Audience Participation

- **Desktops/laptops:** Responsible for or involved in patching 5000 or more, 500, 50
- **Servers:** Responsible for or involved in patching 1000 or more, 100, 10
- **Tools:** What do you use to patch?
- **Timing:** “Patch Tuesday” … 30 days or less, 60 days, 90 days, don’t ask
- **Info:** “In the wild” sources?
- **Life:** Are you happy?

In the News

- **phpMyAdmin XSS Flaws**
  A new version of phpMyAdmin has two serious security holes that could allow attackers to read and cross-site scripting attacks.
  According to an advisory from a vulnerability scanner tool, one of the vulnerabilities is a cross-site scripting attack via a crafted URL that can be exploited by an attacker.
  According to an unpublished reference, a cross-site scripting attack can be used to steal sensitive information.

- **Oracle to Patch 38 Flaws**
  Oracle plans to release an update on Tuesday that will patch 38 vulnerabilities across hundreds of products.
  Oracle’s Critical Patch Update, scheduled for 20 October, contains fixes for numerous flaws, the company said. Many of the security vulnerabilities have the maximum score of 10.0 on the common vulnerability scoring system (CVSS), marking them as critical. For example, vulnerabilities affecting Oracle Core DBMS, Oracle Database and Oracle Network Authentication have received a CVSS score of 10.0.

- **Yada, yada, yada**
Size Matters

- **Enterprise**
  - Complex dependencies
  - Expensive to test and deploy
  - Complicated tools
  - Experienced admins, multiple teams

- **Medium Business**
  - Automated tools
  - Outsourced

- **Small Office/Home Office**
  - Automatic downloads

External Factors

Compliance Issues

**Guidance**
- PCI DSS
- FSMA
- GLBA
- SOX

**Areas**
- Timing
- Testing
- Scanning
- Audit

Requirements Matrix
Policy
Rating the Risk
Am I Hot or Not?

- Bulletin Rating
  - Aggregate across all versions
  - Critical | Important | Moderate | Low
- Per Vulnerability Info
  - Exploitability index
  - Publicly disclosed
  - Is it currently being exploited?
- Any known issues with the fix?
- Deployment Priority

Zero Day Exploits

- Who gets notified?
- Incident response plan
- Impact of mitigations and workarounds
- Full vs Responsible disclosure
Securing the Stack

- OS
- Service Packs
- Runtime environments
- Applications
- Patches
- Backend data systems
  - Data in transit
  - Data at rest
- Partners
- What about the cloud?

Lifecycle Matters

- Mainstream support
- Extended support
- Then what?
- Service pack lifecycle
  - One or two years from release of next SP
    - XP SP3 released 4/21/2008
    - XP SP2 released 9/17/2004, retires 7/13/2010
- www.microsoft.com/lifecycle
- W2K extended support ends July 2010!
## Lifecycle Timeframes

### Service Packs

<table>
<thead>
<tr>
<th>Product Family</th>
<th>12 Months</th>
<th>24 Months</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Microsoft Dynamics SL, Microsoft Dynamics GP, Microsoft Dynamics NAV, Microsoft Dynamics CRM, and, Microsoft Dynamics AX</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Office</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Servers</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Developer Tools</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Business Solutions</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>Consumer, Hardware, Multimedia, Games</td>
<td></td>
<td>Yes</td>
</tr>
</tbody>
</table>

## Downstream Vulnerabilities

- **Visual Studio ATL issue**
  - Created vulnerable software
  - **MS09-035 (July out-of-band release)**
  - Must re-link and redistribute software

- **Weak public key issue**
  - Affected Debian and Ubuntu distributions
  - Debian security advisory DSA-1571-1
  - Must generate and distribute new keys

- **Full magnitude of the exposure may never be known**
Modifying Source Code

- Good idea or bad idea?
- Regressions based on ISV updates
- Core competencies
- Security-trained developers
- passfilt.dll
  - Modify securely
  - Test, test, test
  - Maintain baseline
  - Maintain configuration for ALL DCs

Wrap Up

- Patching is not going away anytime soon, rhythm of the business
- Process beats ad hoc, and should align to policy
- Due diligence and rapid response are not necessarily opposed
- It may be bigger than it first appears
- Tomorrow will bring something new, but something old may come back
Resources

- Best Practices for Applying Service Packs, Hotfixes and Security Patches
- Ten Principles of Microsoft Patch Management
- TechNet Radio: Patch Management at Microsoft
- Security Bulletin Severity Rating System
  http://www.microsoft.com/technet/security/bulletin/rating.mspx
- Microsoft Exploitability Index