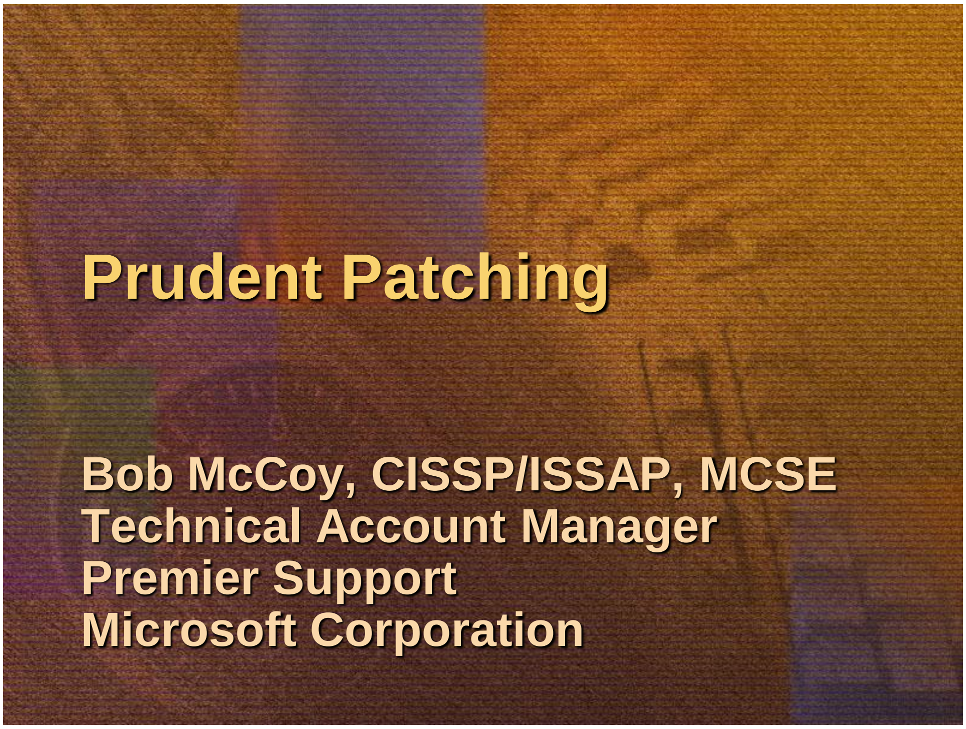
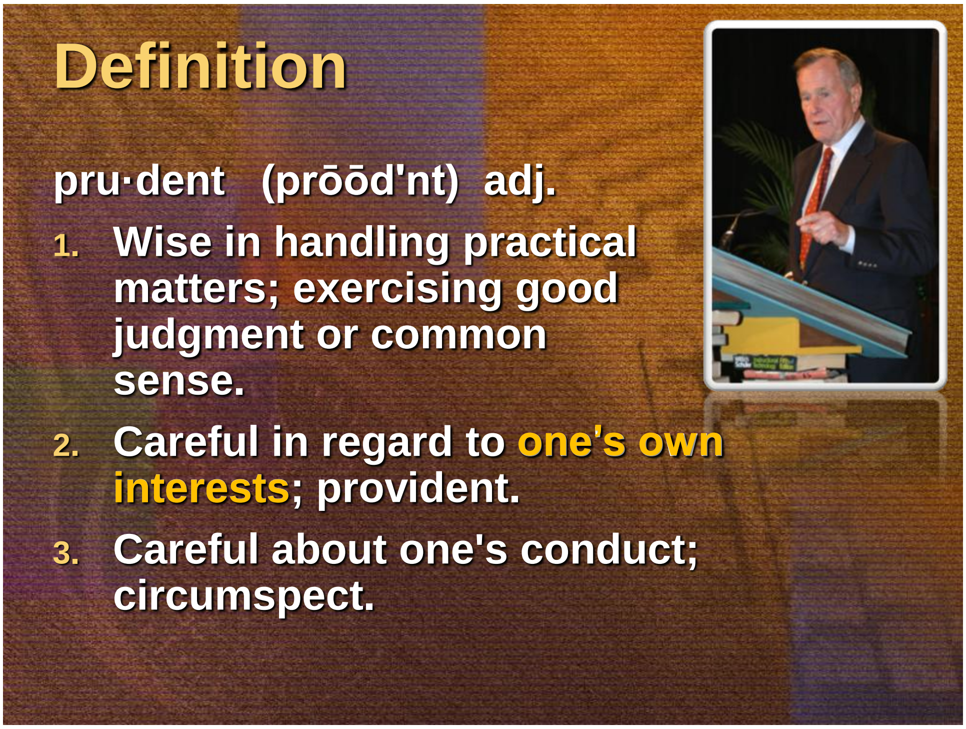


Prudent Patching

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



Definition

pru·dent (prōōd'nt) adj.

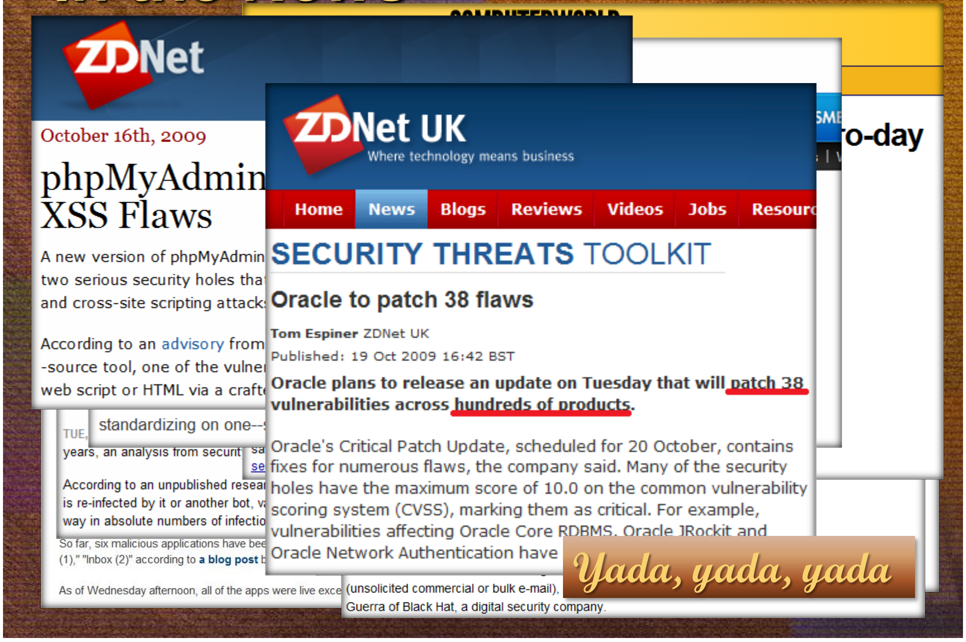
1. Wise in handling practical matters; exercising good judgment or common sense.
2. Careful in regard to one's own interests; provident.
3. Careful about one's conduct; circumspect.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

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



October 16th, 2009

phpMyAdmin
XSS Flaws

A new version of phpMyAdmin
two serious security holes tha
and cross-site scripting attack

According to an advisory from
-source tool, one of the vulne
web script or HTML via a craft

TUE,
standardizing on one--
years, an analysis from securit
sa
se

According to an unpublished resea
is re-infected by it or another bot, v
way in absolute numbers of infectio

So far, six malicious applications have bee
(1)," "Inbox (2)" according to a blog post b

As of Wednesday afternoon, all of the apps were live exce

(unsolicited commercial or bulk e-mail),
Guerra of Black Hat, a digital security company.

SECURITY THREATS TOOLKIT

Oracle to patch 38 flaws

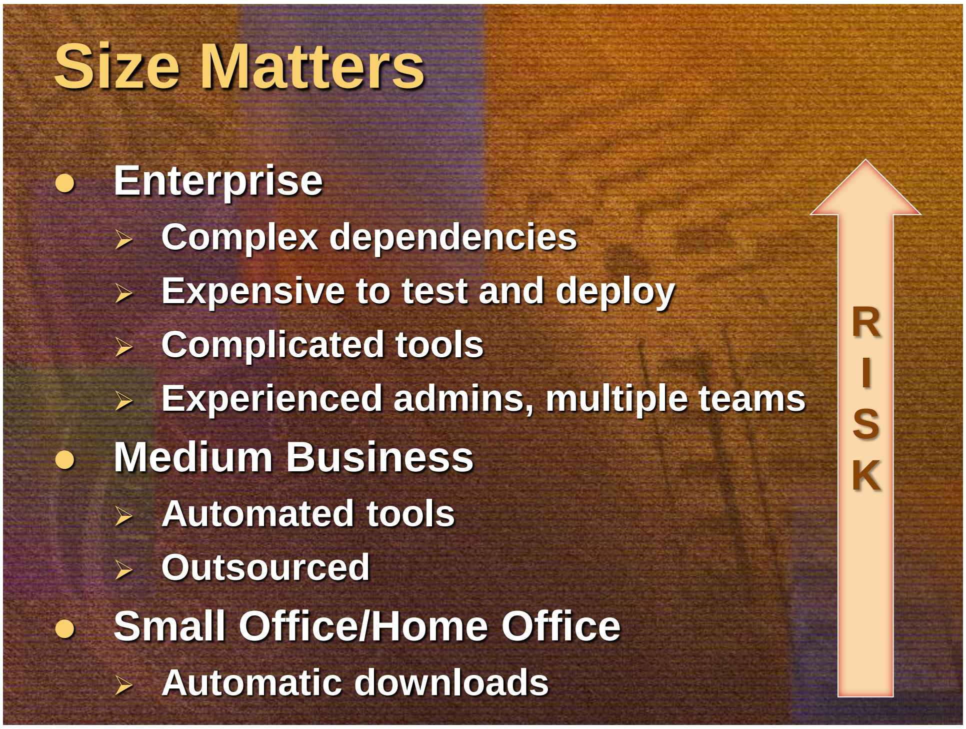
Tom Espiner ZDNet UK
Published: 19 Oct 2009 16:42 BST

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 holes have the maximum score of 10.0 on the common vulnerability scoring system (CVSS), marking them as critical. For example, vulnerabilities affecting Oracle Core RDBMS, Oracle JRockit and Oracle Network Authentication have

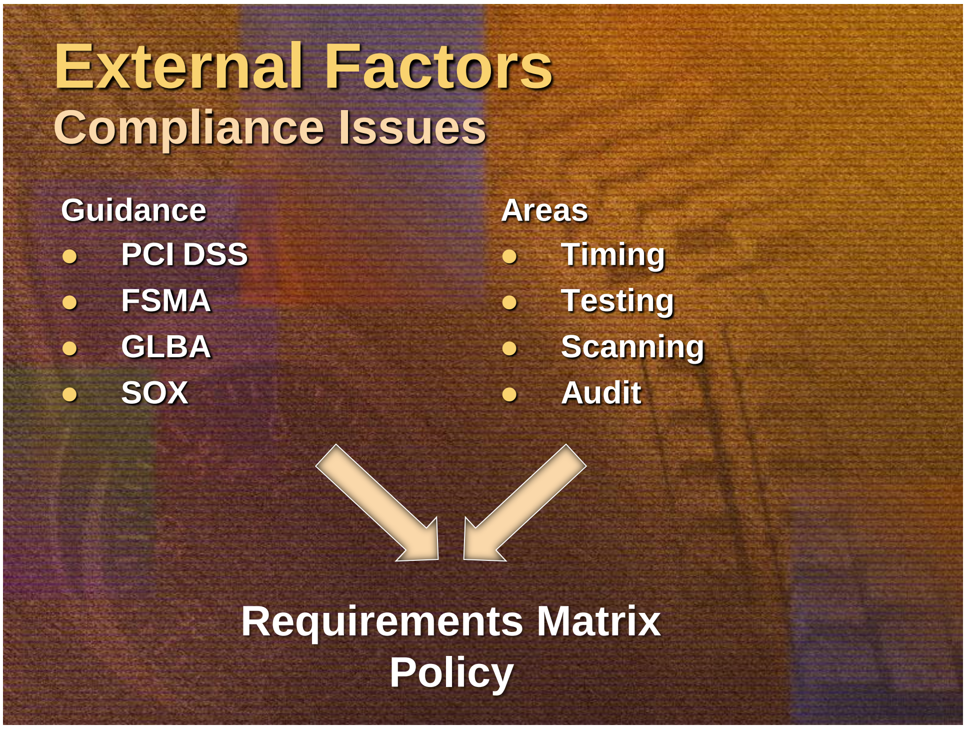
Yada, yada, yada

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



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

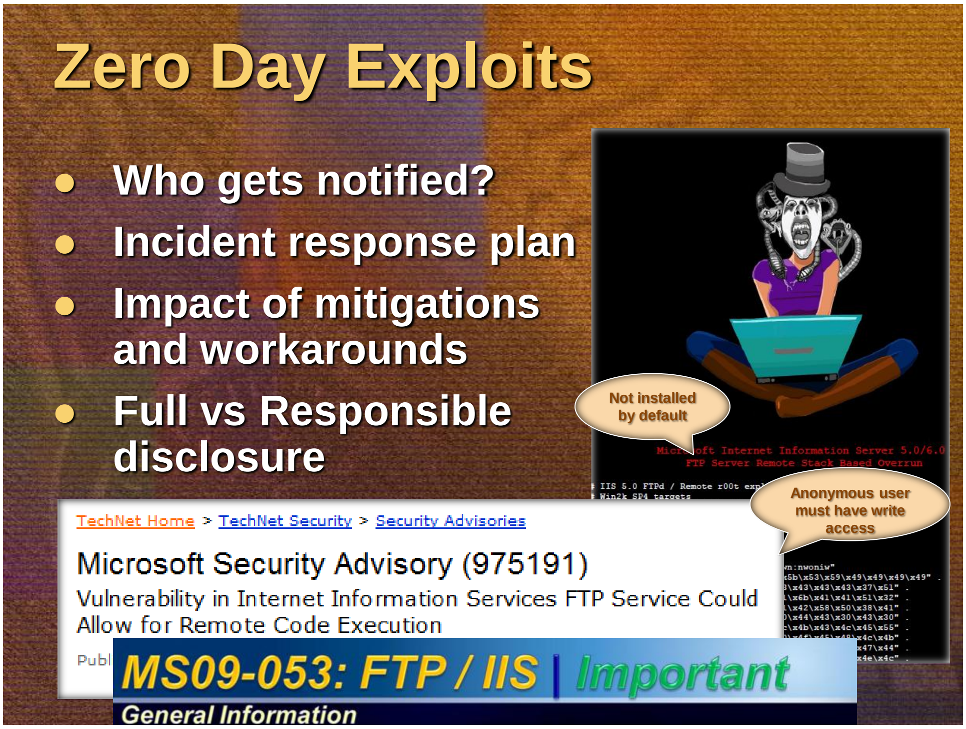
This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

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

```
Microsoft Internet Information Server 5.0/6.0
  FTP Server Remote Stack Based Overrun

# IIS 5.0 FTPd / Remote r00t exp
# Win2k SP4 targets

wn:nwoniw"
x5b\x53\x59\x49\x49\x49\x49" .
3\x43\x43\x43\x37\x51" .
1\x6b\x41\x41\x51\x32" .
1\x42\x58\x50\x38\x41" .
0\x44\x43\x30\x43\x30" .
c\x4b\x43\x4c\x45\x55" .
x4c\x4b" .
x47\x44" .
x4e\x4c" .
```

TechNet Home > TechNet Security > Security Advisories

Microsoft Security Advisory (975191)

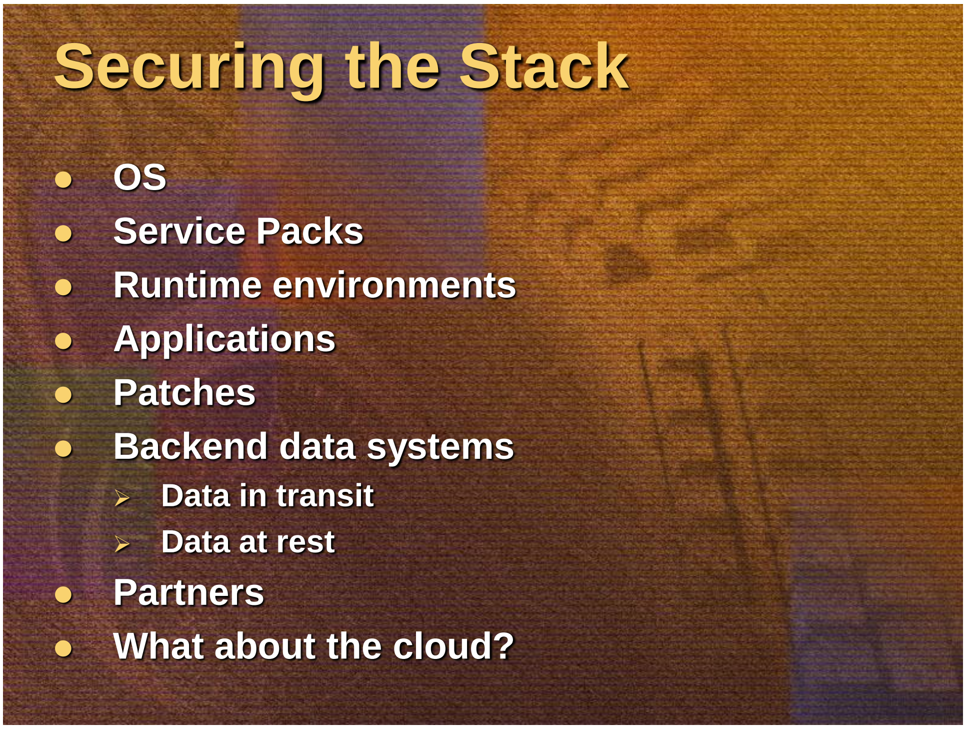
Vulnerability in Internet Information Services FTP Service Could Allow for Remote Code Execution

Publ

MS09-053: FTP / IIS | Important

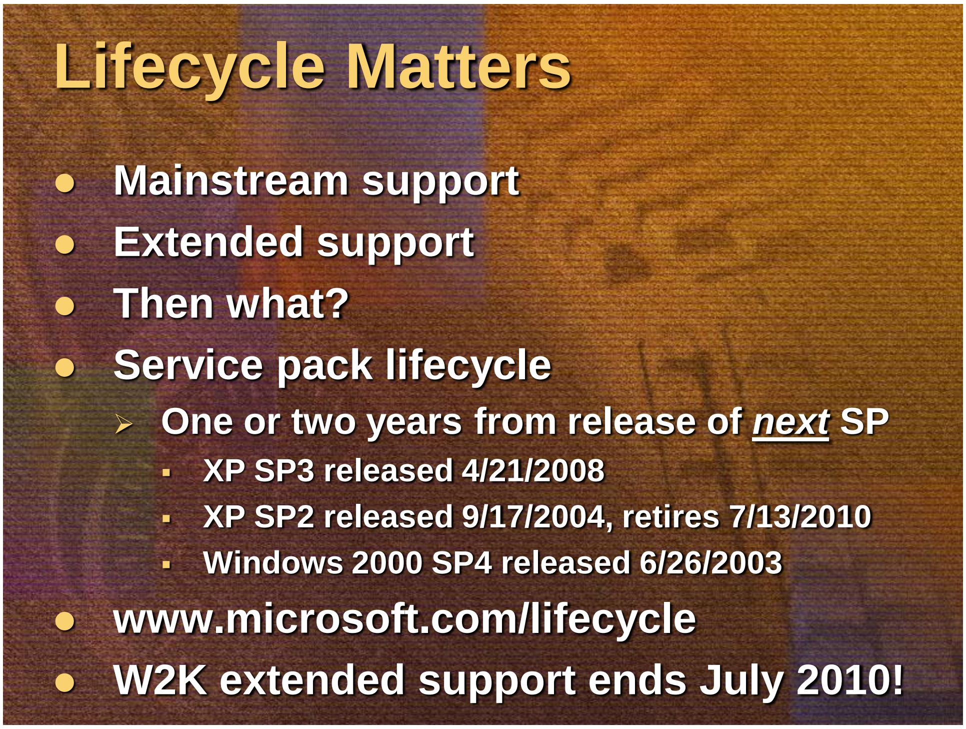
General Information

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



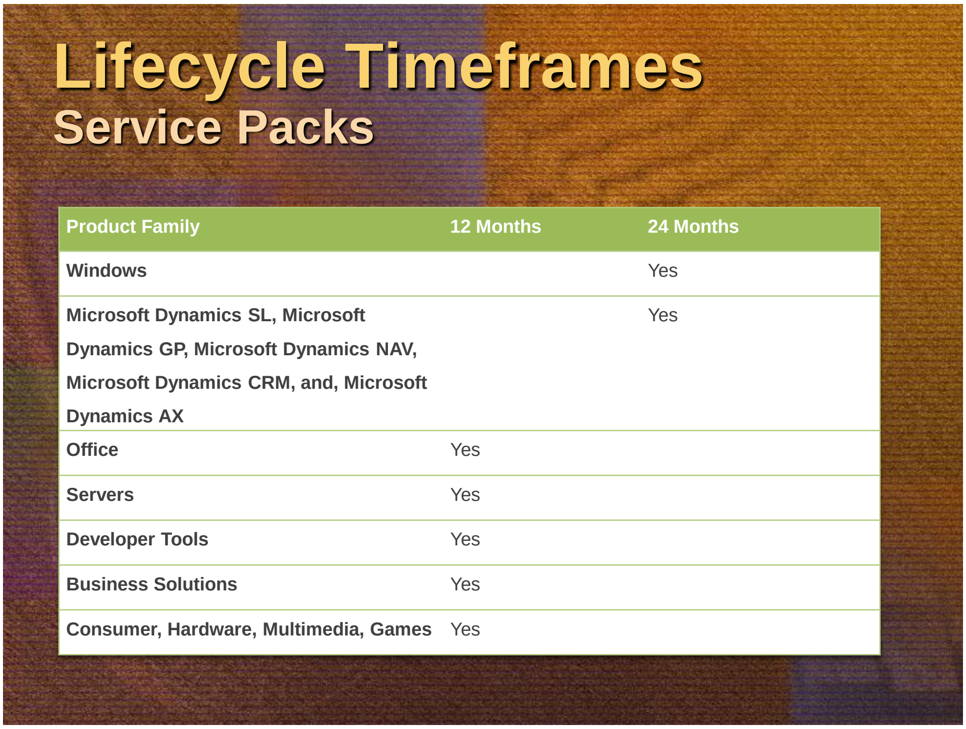
Securing the Stack

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



Lifecycle Matters

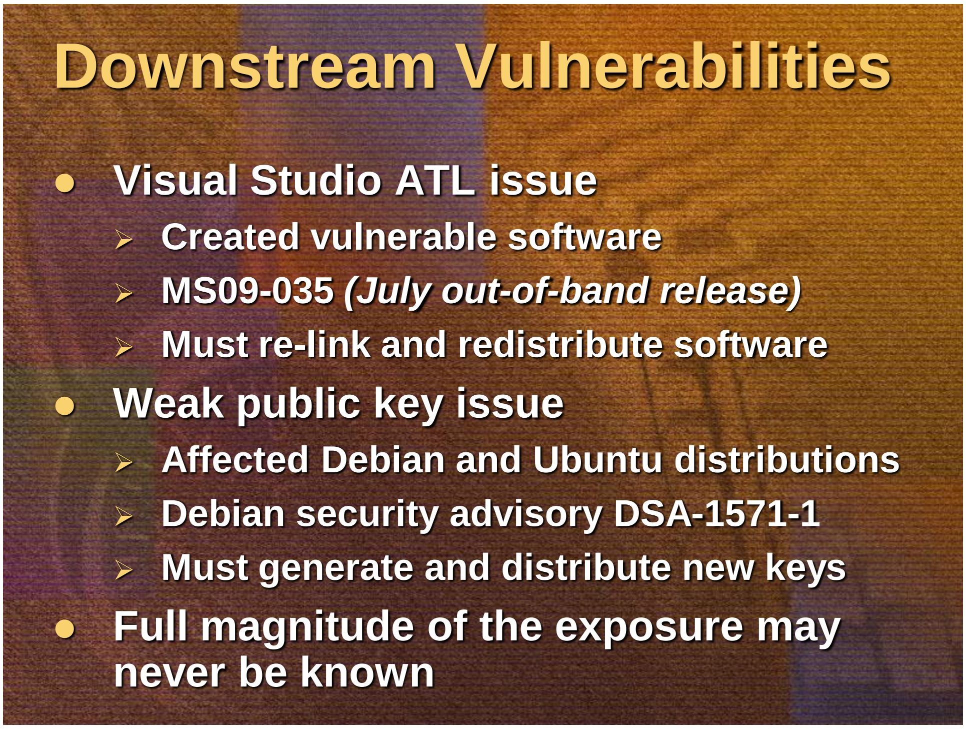
- Mainstream support
- Extended support
- Then what?
- Service pack lifecycle
  - One or two years from release of *next* SP
    - XP SP3 released 4/21/2008
    - XP SP2 released 9/17/2004, retires 7/13/2010
    - Windows 2000 SP4 released 6/26/2003
- www.microsoft.com/lifecycle
- W2K extended support ends July 2010!



Lifecycle Timeframes

Service Packs

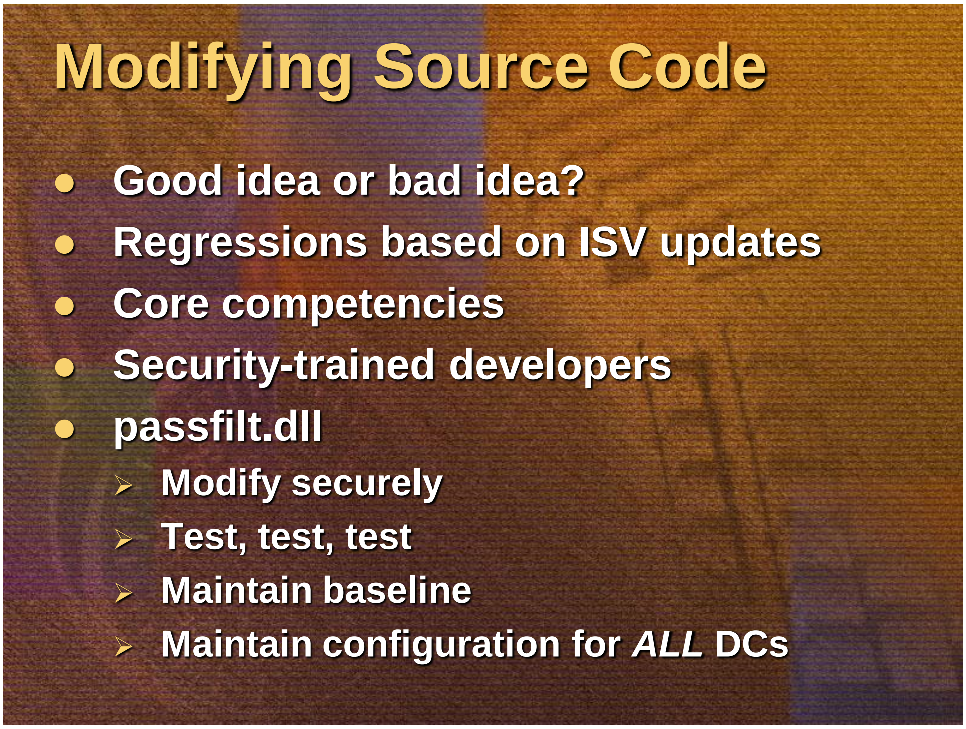
Product Family	12 Months	24 Months
Windows		Yes
Microsoft Dynamics SL, Microsoft Dynamics GP, Microsoft Dynamics NAV, Microsoft Dynamics CRM, and, Microsoft Dynamics AX		Yes
Office	Yes	
Servers	Yes	
Developer Tools	Yes	
Business Solutions	Yes	
Consumer, Hardware, Multimedia, Games	Yes	



Downstream Vulnerabilities

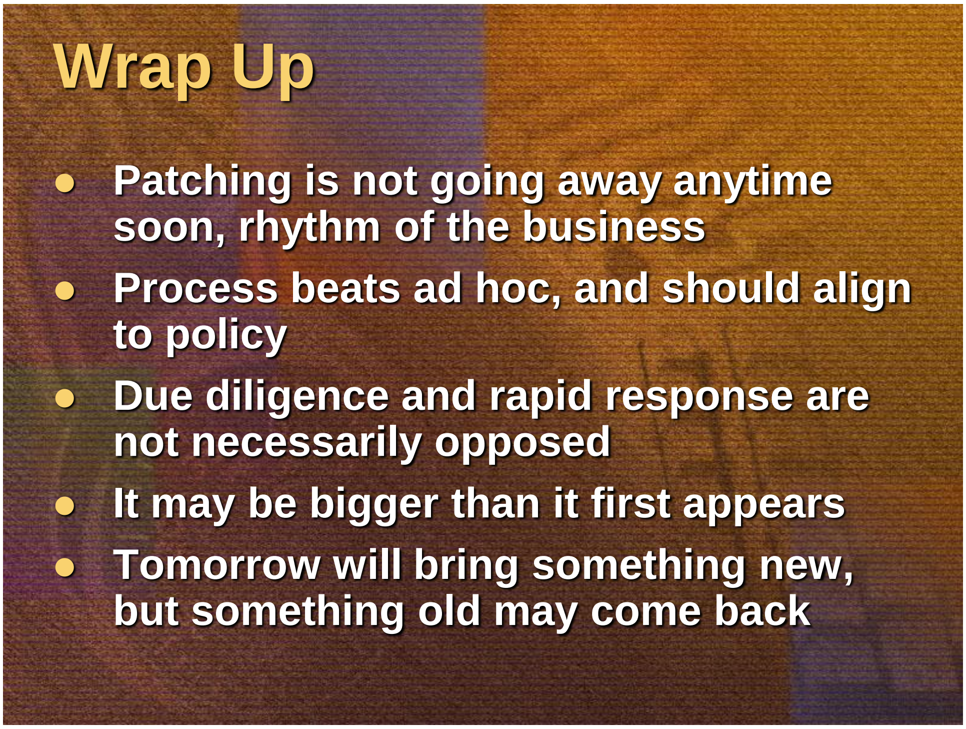
- Visual Studio ATL issue
  - Created vulnerable software
  - MS09-035 *(July out-of-band release)*
  - Must re-link and redistribute software
- Weak public key issue
  - Affected Debian and Ubuntu distributions
  - Debian security advisory DSA-1571-1
  - Must generate and distribute new keys
- Full magnitude of the exposure may never be known

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.



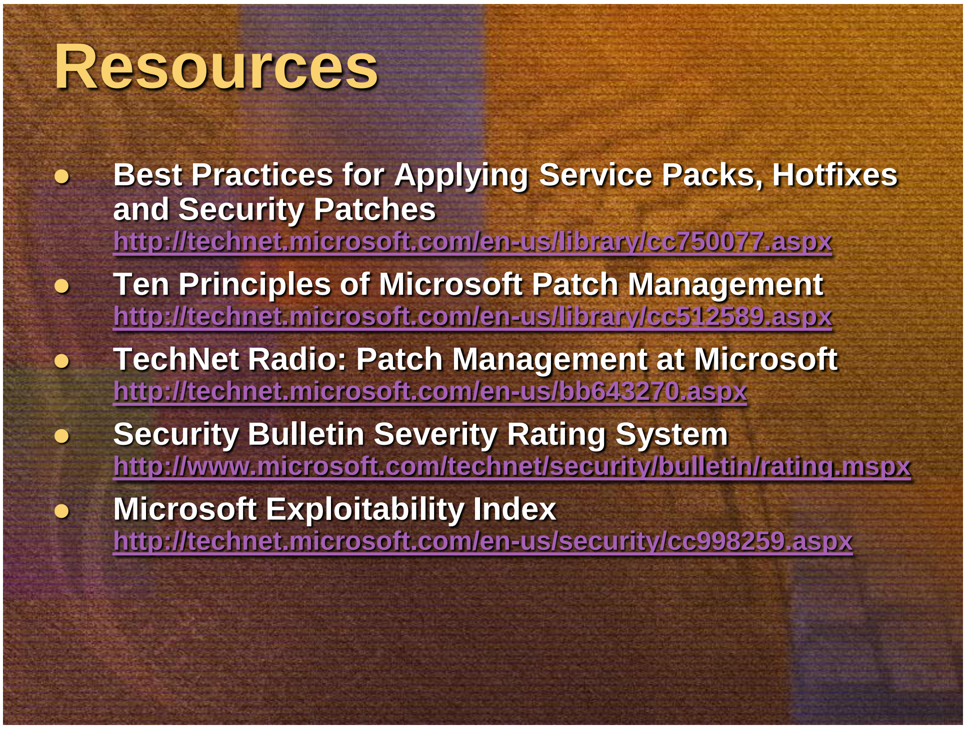
Modifying Source Code

- 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**
  http://technet.microsoft.com/en-us/library/cc750077.aspx
- **Ten Principles of Microsoft Patch Management**
  http://technet.microsoft.com/en-us/library/cc512589.aspx
- **TechNet Radio: Patch Management at Microsoft**
  http://technet.microsoft.com/en-us/bb643270.aspx
- **Security Bulletin Severity Rating System**
  http://www.microsoft.com/technet/security/bulletin/rating.mspx
- **Microsoft Exploitability Index**
  http://technet.microsoft.com/en-us/security/cc998259.aspx

Microsoft®

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.

This presentation is for informational purposes only. Microsoft makes no warranties, express or implied, in this summary.