HELPING SECURE THE PLANET! – NEW STRATEGIC INITIATIVES FROM MICROSOFT TO ROCK YOUR WORLD

Steve Adegbite, Mike Reavey and Katie Moussouris
Microsoft
Commitment to customers & Trustworthy Computing
Threat environment is evolving
Collaboration is key
No one vendor, partner, solution is enough
We’re going to announce 3 programs today that are about protecting customers through collaboration
Agenda

- Microsoft Vulnerability Research
- Microsoft Active Protections Program
- Exploitability Index
Three Take-Aways

- Update Tuesday – Who can protect me?
- Update Tuesday – Which are the most important?
- Beyond Windows – what about all the other applications on my system?
Who can protect me?

Which are the most important?

What about all the other applications on my system?
Who am I? Katie Moussouris

- Microsoft Security Strategist since April 2007
- Founder of Symantec Vulnerability Research
- One of the Artists Formerly Known as @stake
- Former application penetration tester for fun and profit
For years, Microsoft has responsibly reported 3rd party vulnerabilities to affected vendors.

Microsoft Vulnerability Research (MSVR) is a new program to formalize and go public with our work in these areas.
You’re Nuts!!

- ...and you’ll never get away with it!!
- Actually, our customers told us to do it (we heard voices)
- Challenges = opportunities
Browser Exploits on XP

- MS 81%
- 3rdParty 19%
Browser Exploits on Vista

3rdParty 92%

MS 8%
Call Me Trimtab

- A small rudder can turn the path of giant ships
- The ship could be just Microsoft, or it can extend to the entire ecosystem
- Is it so crazy to want to unite, like countries of the world fighting an alien invasion?
MSVR Goooodd!!!

- Proactive protection of customers on our platform
- Work with other vendors to improve security for all
- Evolve our security practices with the customer in mind
Begin with 3rd party vendors with the broadest impact to our customers

Collect ongoing field data to spot trends in order to determine when and how to expand
MSVR Sources

- From within Microsoft
  - Vulns found through the use of our SDL tools
  - Vulns found by individuals within our security teams
- From external finders
  - Researchers who thought they were reporting a Microsoft issue that turns out to be a 3rd party issue
  - Researchers who report blended threats involving both MS and 3rd party issues
MSVR and You

- **How will I notice?**
  - More secure platform
  - 3rd party vendor acknowledgement

- **How can I participate?**
  - Try the affected 3rd party vendor first ;-) 
  - If you need help, talk to us at msvr@microsoft.com

As always, report Microsoft vulnerabilities to us at secure@microsoft.com
The hard questions:

- When’s it going to start?
  - It has already begun!

- Why don’t you just mind your own (buggy) business?
  - We hope to continue to improve ourselves, while helping others and learning from them as well – co-opetition!
  - Customers come first, and this is the next leap in the security industry’s evolution

- Who are you looking at?
  - We gather feedback from customer data on which 3rd party software is installed most on the Windows platform.
Next Up: More Evolution with Steve
Sound off
Who am I?

Steve Adegbite
Sr. Program Mgr Lead

- Microsoft since Jan 2006
- Government/Contractor CNO cyber specialist
- Founder of USMC Information Assurance Red Team (MCIART)
- Former USMC Computer Emergency Response Team (MAR-CERT) officer-in-charge
What is the Microsoft Active Protections Program?

- New Program to Share info in advance of monthly release of security updates
- Designed to give defenders a head start in the race between exploit and protection availability
- Shared with vetted participating members
High Noon is 10:00am PST...

- Predictable monthly security update cycle
  - Malware authors take advantage of this
- Changing threat environment
- Instant security update deployment does not happen everywhere
  - Most test security updates prior to deployment
  - After 10AM, exploit code is becoming increasingly available
- Example: Immunity’s MS08-025 exploit code
Microsoft Security Bulletin MS08-025 – Important Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)

Published: April 8, 2008  Updated: April 11, 2008

General Information

Executive Summary
This security update resolves a privately reported vulnerability in the Windows kernel. A local attacker who successfully exploited this vulnerability could take complete control of an affected system. An attacker could then install programs; view, change, or delete data; or create new accounts.

This is an important security update for all supported editions of Windows 2000, Windows XP, Windows Server 2003, Windows Vista and Windows Server 2008. For more information, see the subsection, Affected and Non-Affected Software, in this section.

This security update addresses the vulnerability by modifying the way that the Windows kernel validates inputs passed from user mode. For more information about this vulnerability, see the Frequently Asked Questions (FAQ) subsection under the next section, Vulnerability Information.

Recommendation. Microsoft recommends that customers apply the update at the earliest opportunity.

Known Issues. Microsoft Knowledge Base Article 911492 documents the currently known issues that customers may experience when they uninstall this security update.

Affected and Non-Affected Software
The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Maximum Security Impact</th>
<th>Aggregate Severity Rating</th>
<th>Bulletins Replaced by this Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Windows 2000 Service Pack 4</td>
<td>Elevation of Privilege</td>
<td>Important</td>
<td>None</td>
</tr>
<tr>
<td>Windows XP Service Pack 2</td>
<td>Elevation of Privilege</td>
<td>Important</td>
<td>None</td>
</tr>
<tr>
<td>Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2</td>
<td>Elevation of Privilege</td>
<td>Important</td>
<td>None</td>
</tr>
<tr>
<td>Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2</td>
<td>Elevation of Privilege</td>
<td>Important</td>
<td>None</td>
</tr>
<tr>
<td>Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP1 for Itanium-based Systems</td>
<td>Elevation of Privilege</td>
<td>Important</td>
<td>None</td>
</tr>
<tr>
<td>Windows Vista and Windows Vista Service Pack 1</td>
<td>Elevation of Privilege</td>
<td>Important</td>
<td>None</td>
</tr>
<tr>
<td>Windows Vista x64 Edition and Windows Vista x64 Edition</td>
<td>Elevation of Privilege</td>
<td>Important</td>
<td>None</td>
</tr>
</tbody>
</table>
Can You Say Big Red Button?
So easy a child could do it....

Node Tree
Exploit Description

WIN32K CLIENTLOADMENU PRIVILEGE ESCALATION
Vulnerability in Windows Kernel Could Allow Elevation of Privilege

ARCH: ['Windows', 'VISTA', '2008']
MSADV: MS08-025
SITE: Local
TYPE: Exploit
CVE NAME: CVE-2008-1084
REPEATABILITY: One Shot
CVSS URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?
cve=CVE-2008-1084
DATE PUBLIC: 04/08/2008

Listener Shell

whoami

All commands to be ran are located here

(CANVAS)$ver
Microsoft Windows [Version 6.0.6001]
(CANVAS)$whoami
win-r3dofbz4jsz\dave
(CANVAS)$whoami
ht authenti\system
It’s the old defend the castle and all of the mouse holes game-attackers know this and use it to their advantage
Time for a New Paradigm…
Community Based Defense

- Change the game
  - Defenders need to get faster.
  - Attackers share. So should we.
  - We need to create a program that has us working collaboratively…
  - Like…
MAPP

Take the Red Pill...
Who Can Join…

- Open to Commercial Vendors
- Vendors must create active protections
- Must have a significant Microsoft customer base
- NDA w/ Microsoft
- Cannot be a seller of product(s) used to attack
- Full criteria will be posted online:
  - [http://www.microsoft.com/presspass/events/blackhat/default.mspx](http://www.microsoft.com/presspass/events/blackhat/default.mspx)

- To find out more (and to apply)
  - email mapp@microsoft.com
Where are the goods man!...

- Demo of MS08-025

Shout out to Bruce Dang...Go see his talk at 16:45 in Augustus 3/4
Come on.. Why is Microsoft Really Doing This?

Microsoft wants to better protect our mutual customers

Security is an ecosystem concern ..why not arm the people that can help with the right information?
What do customers really get out of this?

- A coalition around defense
- New partners in their fight against exploits
- An industry working in a swifter and more proactive manner for our customers

Skeptical, eh?
The hard questions:

- When’s it going to start?
  - October 2008

- Are you worried about someone leaking vulnerability information?
  - The benefits outweigh the risk
  - Safeguard measures have been put in place.

- What if you don’t let my favorite product company participate?
  - We are doing everything possible to get the right people in
  - We continually review our processes to better meet customer needs
Who am I? **Mike Reavey**

- MSRC since 2003
  - Blaster, Sasser, Zotob
- PenTesting Air Force networks prior to that
- Securing/Optimizing prior networks prior to that
- Managing a Air Force network prior to that
Predicting the Future: Exploitability Index (XI)

MAPP
• How Microsoft shares information to help ensure customers are secure even without updates

Exploitability Index
• Helps customers prioritize updates and provides more information to make assessments
What is Exploitability Index?

- Additional information to help customers prioritize the security updates
- Designed to give guidance on likelihood of functional exploit
- Released each month as part of a Security Bulletin Summary from Microsoft
- Developed based on watching trends in the ecosystem
Customer Situation:
Updating is still difficult, and there’s still the “race condition”

Reality:
While we answer this question in the bulletins today, it frequently changes within the first two weeks (sometimes two hours) after release.

GOAL: Prediction of the Likelihood that Functional Exploit code will be released.

Exploitability Index (XI)
Evaluate exploitability of the vulnerabilities using industry methodology and MAPP partners.

Provide a prediction of Likelihood of Exploitation for each Vulnerability

“Is there exploit code available?”
Microsoft Vulnerability Exploit Details

Trends

- 2006: 29% of Microsoft vulnerabilities had public exploit code
- 2007: 21% of Microsoft vulnerabilities had public exploit code
How are you making these predictions?
How's it different than...

- Bulletin Severity Ratings
- CVSS
A vulnerability whose exploitation could allow the propagation of an Internet worm without user action

A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users data, or of the integrity or availability of processing resources

Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation

A vulnerability whose exploitation is extremely difficult, or whose impact is minimal

Bulletin Ratings Assume a Determined and Skilled attacker
So what does it look like?

Published: April 8, 2008 | Updated: April 16, 2008

Version: 1.2
This bulletin summary lists security bulletins released for April 2008.

With the release of the bulletins for April 2008, this bulletin summary replaces the bulletin advance notification originally issued April 3, 2008. For more information about the bulletin advance notification service, see Microsoft Security Bulletin Advance Notification.

For information about how to receive automatic notifications whenever Microsoft security bulletins are issued, visit Microsoft Technical Security Notifications.

Microsoft is hosting a webinar to address customer questions on these bulletins on April 9, 2008, at 11:00 AM Pacific Time (US & Canada). Register now for the April Security Bulletin Webcast. After this date, the webinar is available on-demand. For more information, see Microsoft Security Bulletin Summaries and Webcasts.

Microsoft also provides information to help customers prioritize monthly security updates with any non-security, high-priority updates that are being released on the same day as the monthly security updates. Please see the section, Other Information.

Bulletin Information

Executive Summaries
The security bulletins for this month are as follows, in order of severity:

- Critical (5)
- Important (3)

Affected Software and Download Locations
How do I use this table?

Use this table to learn about the security updates that you may need to install. You should review each software program or component listed to see whether any security updates are required. If a software program or component is listed, then the available software update is hyperlinked and the severity rating of the software update is also listed.

Note: You may have to install several security updates for a single vulnerability. Review the whole column for each bulletin identifier that is listed to verify the updates that you have to install, based on the programs or components that you have installed on your system.

Windows Operating System and Components

<table>
<thead>
<tr>
<th>Microsoft Windows 2000</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bulletin Identifier</td>
</tr>
</tbody>
</table>
Exploitability Index

How do I use this table?

Use this table to learn about the likelihood of exploit code to be released for each of the security updates that you may need to install. You should review each of the predications below, in combination with your specific configuration in order to prioritize your deployment. For more information about what these ratings mean, and how they are determined, please visit the Microsoft Exploit Index Overview Page.

<table>
<thead>
<tr>
<th>Bulletin ID</th>
<th>Bulletin Title</th>
<th>CVEID</th>
<th>Exploitability Prediction</th>
<th>Key Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS08-021</td>
<td>Vulnerabilities in GDI Could Allow Remote Code Execution (948590)</td>
<td>CVE-2008-1087</td>
<td>Consistent Exploit Code Likely</td>
<td>Windows 2000 Service Pack 4 at High Likelihood; other Operating Systems at Medium</td>
</tr>
<tr>
<td>MS08-025</td>
<td>Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)</td>
<td>CVE-2008-1084</td>
<td>Consistent Exploit Code Likely</td>
<td>All Operating Systems at High Likelihood</td>
</tr>
<tr>
<td>MS08-018</td>
<td>Vulnerability in Microsoft Project Could Allow Remote Code Execution (950183)</td>
<td>CVE-2008-1085</td>
<td>Inconsistent Exploit Code Possible</td>
<td></td>
</tr>
<tr>
<td>MS08-019</td>
<td>Vulnerabilities in Microsoft Vista Could Allow Remote Code Execution (944067)</td>
<td>CVE-2008-1089</td>
<td>Inconsistent Exploit Code Possible</td>
<td></td>
</tr>
</tbody>
</table>
### Understanding the Index

<table>
<thead>
<tr>
<th>Bulletin ID</th>
<th>Bulletin Title</th>
<th>CVEID</th>
<th>Exploitability Prediction</th>
<th>Key Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS08-021</td>
<td><strong>Vulnerabilities in GDI Could Allow Remote Code Execution (948590)</strong></td>
<td>CVE-2008-1087</td>
<td>Consistent Exploit Code Likely</td>
<td>Windows 2000 Service Pack 4 at High Likelihood; other Operating Systems at Medium</td>
</tr>
</tbody>
</table>

Consistent Exploit Code Likely

Inconsistent Exploit Code Likely

Functioning Exploit Code Unlikely
<table>
<thead>
<tr>
<th>Bulletin Number</th>
<th>Bulletin Name</th>
<th>Release Date</th>
<th>CVE</th>
<th>Severity</th>
<th>Exploitability Prediction</th>
<th>Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS08-030</td>
<td>Bluetooth</td>
<td>6/10/2008</td>
<td>CVE-2008-1453</td>
<td>Critical</td>
<td>Inconsistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-022</td>
<td>Script</td>
<td>4/8/2008</td>
<td>CVE-2008-0083</td>
<td>Critical</td>
<td>Inconsistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-032</td>
<td>ActiveX</td>
<td>6/10/2008</td>
<td>CVE-2007-0675</td>
<td>Functioning Exploit Code Unlikely</td>
<td>Correct</td>
<td></td>
</tr>
<tr>
<td>MS08-037</td>
<td>DNS</td>
<td>7/8/2008</td>
<td>CVE-2008-1447</td>
<td>Important</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-031</td>
<td>Internet Explorer</td>
<td>6/10/2008</td>
<td>CVE-2008-1544</td>
<td>Important</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-031</td>
<td>Internet Explorer</td>
<td>6/10/2008</td>
<td>CVE-2008-1442</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-023</td>
<td>DirectX</td>
<td>6/10/2008</td>
<td>CVE-2008-0011</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-033</td>
<td>WMP</td>
<td>6/10/2008</td>
<td>CVE-2008-1444</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-021</td>
<td>GDI32</td>
<td>4/8/2008</td>
<td>CVE-2008-1087</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-025</td>
<td>Win32</td>
<td>4/8/2008</td>
<td>CVE-2008-1084</td>
<td>Important</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-017</td>
<td>OWC</td>
<td>3/11/2008</td>
<td>CVE-2007-1201</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-017</td>
<td>OWC</td>
<td>3/11/2008</td>
<td>CVE-2006-4695</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>Correct</td>
</tr>
<tr>
<td>MS08-019</td>
<td>Visio</td>
<td>4/8/2008</td>
<td>CVE-2008-1090</td>
<td>Important</td>
<td>Inconsistent Exploit Code Likely</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-037</td>
<td>DNS</td>
<td>7/8/2008</td>
<td>CVE-2008-1454</td>
<td>Important</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-038</td>
<td>Explorer</td>
<td>7/8/2008</td>
<td>CVE-2008-1435</td>
<td>Important</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-040</td>
<td>SQL Page Reuse</td>
<td>7/8/2008</td>
<td>CVE-2008-0085</td>
<td>Important</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-040</td>
<td>SQL MemCorruption</td>
<td>7/8/2008</td>
<td>CVE-2008-0107</td>
<td>Important</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-034</td>
<td>WINS</td>
<td>6/10/2008</td>
<td>CVE-2008-1451</td>
<td>Important</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-036</td>
<td>Word</td>
<td>5/13/2008</td>
<td>CVE-2008-0134</td>
<td>Critical</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-027</td>
<td>Publisher</td>
<td>5/13/2008</td>
<td>CVE-2008-0119</td>
<td>Critical</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-020</td>
<td>DNS</td>
<td>4/8/2008</td>
<td>CVE-2008-0087</td>
<td>Important</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-021</td>
<td>GDI32</td>
<td>4/8/2008</td>
<td>CVE-2008-1083</td>
<td>Critical</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-023</td>
<td>Killbit</td>
<td>4/8/2008</td>
<td>CVE-2008-1086</td>
<td>Critical</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-024</td>
<td>IE</td>
<td>4/8/2008</td>
<td>CVE-2008-1085</td>
<td>Critical</td>
<td>Inconsistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Excel</td>
<td>3/11/2008</td>
<td>CVE-2008-0112</td>
<td>Important</td>
<td>Functioning Exploit Code Unlikely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-035</td>
<td>NTDSA DoS</td>
<td>6/10/2008</td>
<td>CVE-2008-1445</td>
<td>Important</td>
<td>Functioning Exploit Code Unlikely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-036</td>
<td>PGM DoS</td>
<td>6/10/2008</td>
<td>CVE-2008-1440</td>
<td>Important</td>
<td>Functioning Exploit Code Unlikely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-036</td>
<td>PGM DoS</td>
<td>6/10/2008</td>
<td>CVE-2008-1441</td>
<td>Important</td>
<td>Functioning Exploit Code Unlikely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-026</td>
<td>Word</td>
<td>5/13/2008</td>
<td>CVE-2008-1091</td>
<td>Critical</td>
<td>Functioning Exploit Code Unlikely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Excel</td>
<td>3/11/2008</td>
<td>CVE-2008-0114</td>
<td>Critical</td>
<td>Functioning Exploit Code Unlikely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-039</td>
<td>OWA</td>
<td>7/8/2008</td>
<td>CVE-2008-2247</td>
<td>Important</td>
<td>Consistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-039</td>
<td>OWA</td>
<td>7/8/2008</td>
<td>CVE-2008-2248</td>
<td>Important</td>
<td>Consistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-040</td>
<td>SQL BO</td>
<td>7/8/2008</td>
<td>CVE-2008-0086</td>
<td>Important</td>
<td>Consistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-040</td>
<td>SQL BO</td>
<td>7/8/2008</td>
<td>CVE-2008-0106</td>
<td>Important</td>
<td>Consistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Excel</td>
<td>3/11/2008</td>
<td>CVE-2008-0111</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Excel</td>
<td>3/11/2008</td>
<td>CVE-2008-0081</td>
<td>Critical</td>
<td>Consistent Exploit Code Likely</td>
<td>None Posted</td>
</tr>
<tr>
<td>MS08-019</td>
<td>Visio</td>
<td>4/8/2008</td>
<td>CVE-2008-1089</td>
<td>Important</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-029</td>
<td>Malware Engine</td>
<td>5/13/2008</td>
<td>CVE-2008-1437</td>
<td>Important</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-029</td>
<td>Malware Engine</td>
<td>5/13/2008</td>
<td>CVE-2008-1438</td>
<td>Important</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-018</td>
<td>Project</td>
<td>4/8/2008</td>
<td>CVE-2008-1088</td>
<td>Critical</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Excel</td>
<td>3/11/2008</td>
<td>CVE-2008-0116</td>
<td>Critical</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Excel</td>
<td>3/11/2008</td>
<td>CVE-2008-0117</td>
<td>Critical</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Excel</td>
<td>3/11/2008</td>
<td>CVE-2008-0115</td>
<td>Critical</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-014</td>
<td>Office</td>
<td>3/11/2008</td>
<td>CVE-2008-0113</td>
<td>Critical</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-016</td>
<td>Office</td>
<td>3/11/2008</td>
<td>CVE-2008-0118</td>
<td>Critical</td>
<td>Not Analyzed</td>
<td>N/A</td>
</tr>
<tr>
<td>MS08-028</td>
<td>Word and Access</td>
<td>5/13/2008</td>
<td>CVE-2007-6026</td>
<td>Important</td>
<td>Public At Release</td>
<td>N/A</td>
</tr>
</tbody>
</table>
The hard questions:

- When’s it going to start?
  - October 2008

- Are you worried about increasing exploitation?
  - “update Tuesday, exploit Wednesday”
  - Giving customers more information is not a bad thing / BUT we’re not giving a cook-book.

- What if you’re wrong?
  - It is risky (MS08-001 IGMP), but customers are asking for it & the methodology is from the community
  - We’re not going alone – MAPP members can comment as well.
Summary

- All of these programs work in concert to provide defense in depth
- MSVR – helps windows platform get more secure
- MAPP – shares information so customers are protected without updates
- XI – helps customers apply most important updates first
3 things to take away

• Update Tuesday – who can protect me?
  • MAPP increases the number of protectors, ready at 10:01 AM
• Update Tuesday – which are the most important?
  • XI provides more information to help customers perform risk assessment
• Beyond Windows – what about all the other stuff on my system?
  • MSVR takes security beyond corporate borders to third party software
For more information

- mapp@microsoft.com
- secure@microsoft.com
- msvr@microsoft.com
- MSRC Ecosystem Strategy Team Blog