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

Steve Adegbite, Mike Reavey and Katie Moussouris
Microsoft

Why Are We Here?

- 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 trough 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?

Three Take-Aways

Update Tuesday

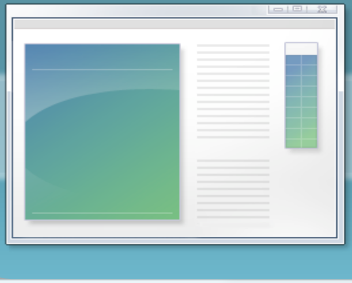
Who can protect me?

Update Tuesday

Which are the most important?

Beyond Windows

What about all the other applications on my system?



Who 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

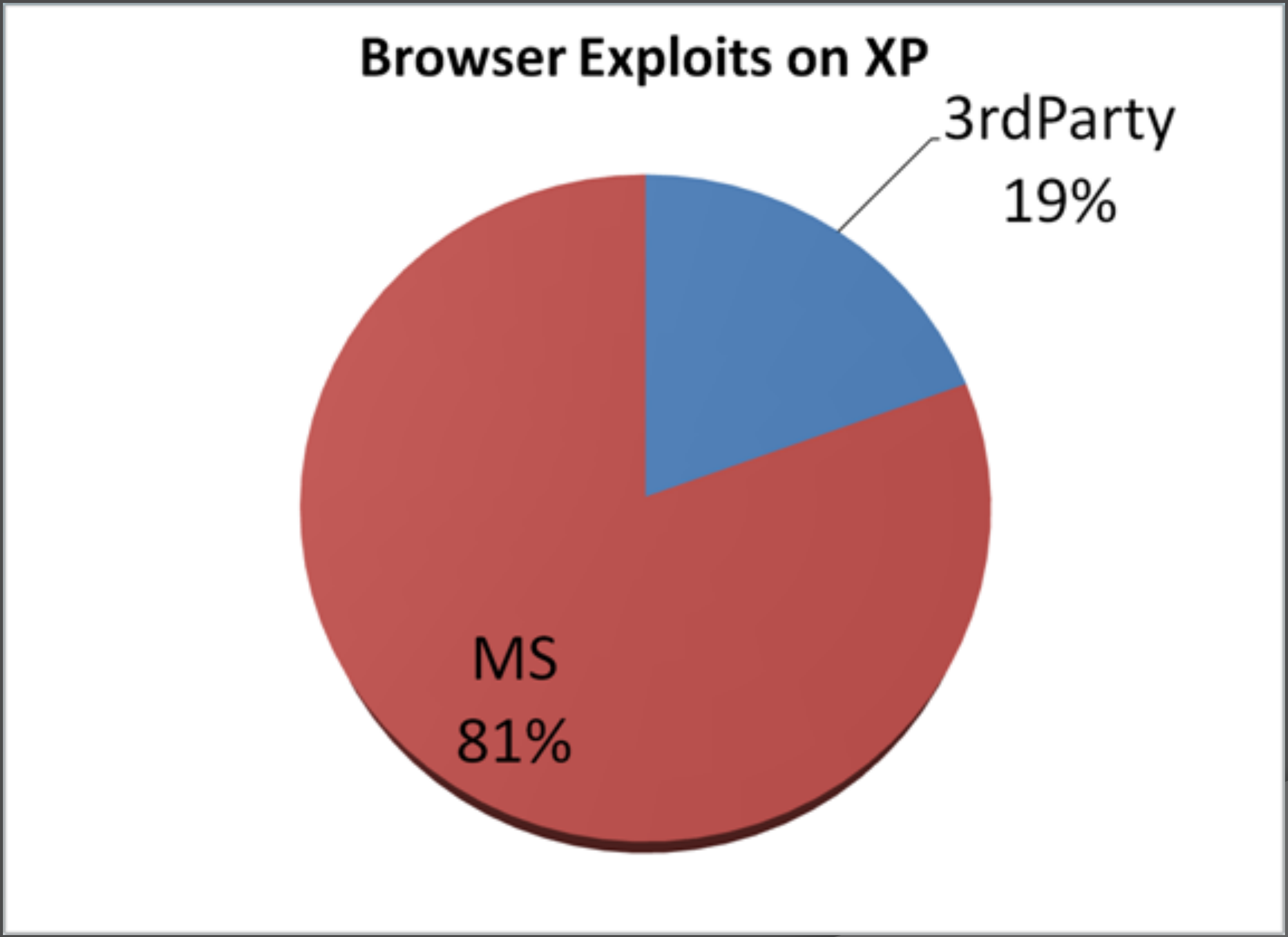
MSVR Bird's Eye View

- 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

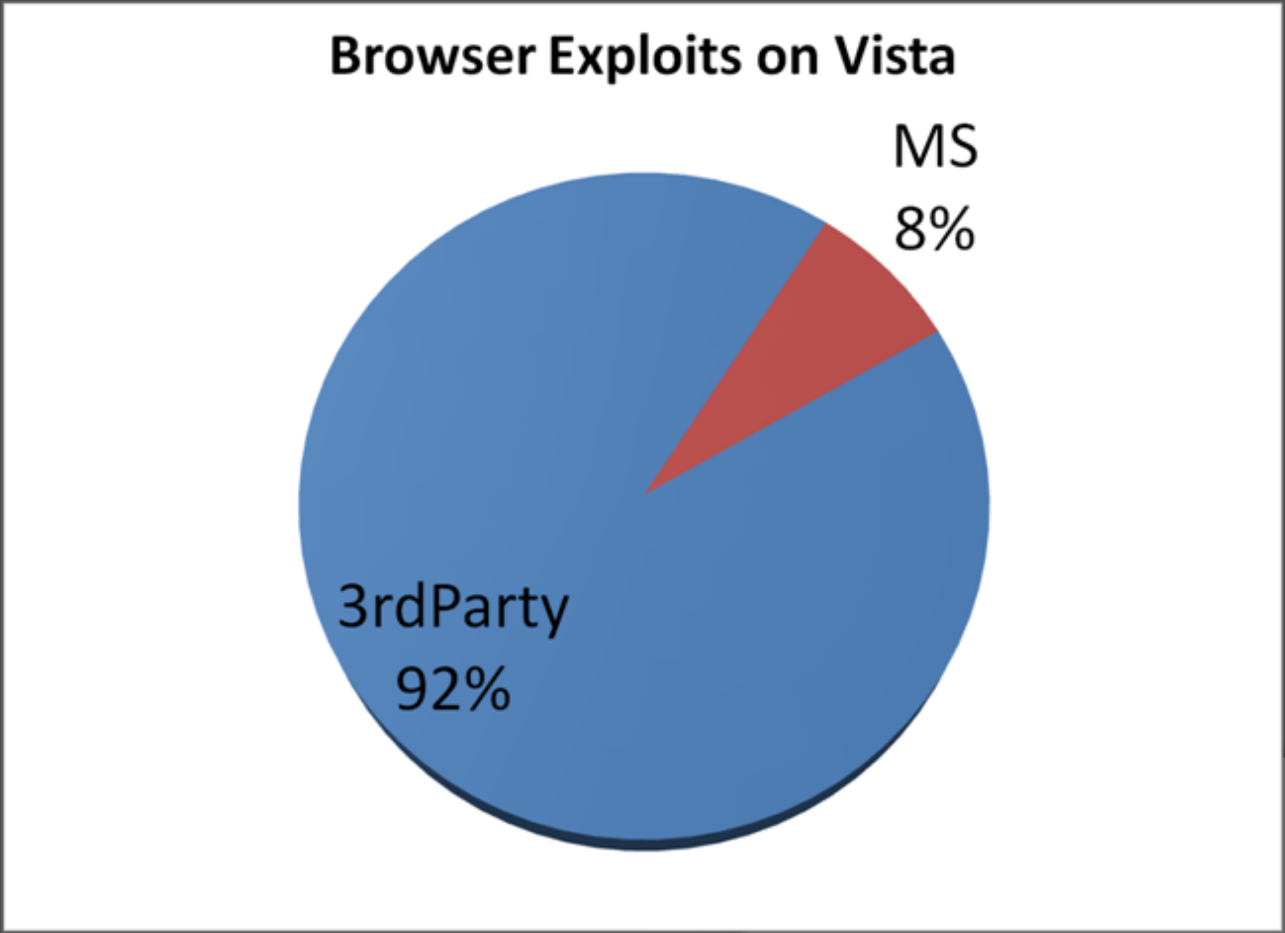
You’re Nuts!!

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

Pac Man/Not Pac Man



Ms. Pac Man/Not Ms. Pac Man



Call Me Trimtab

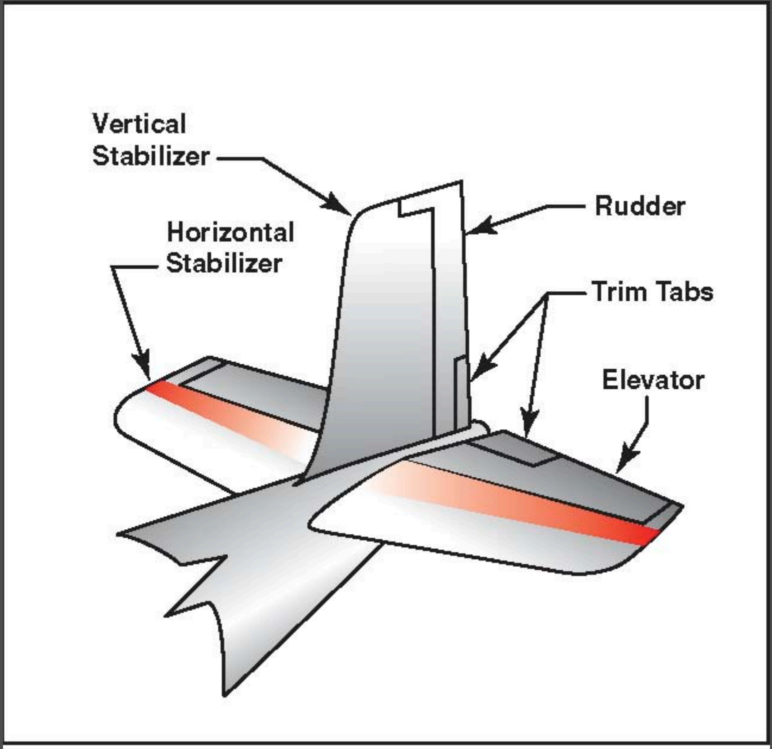
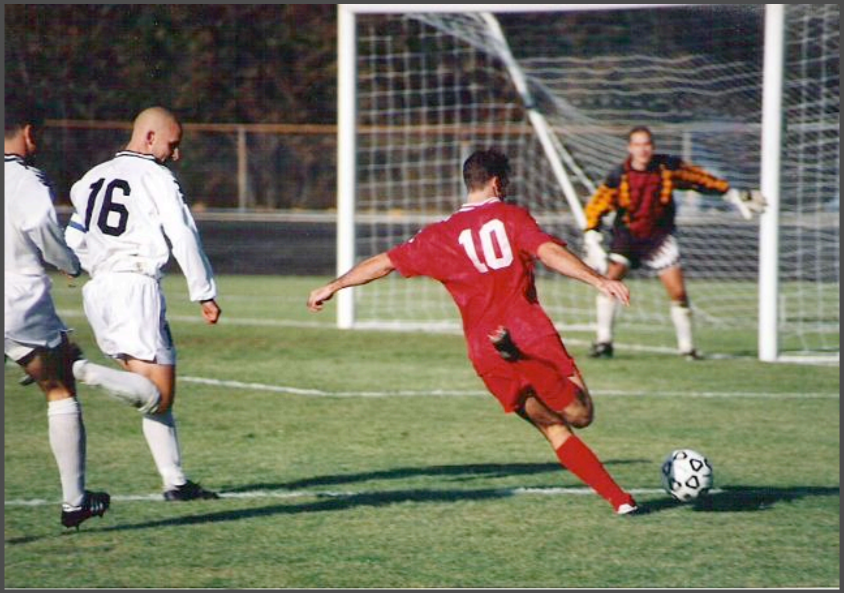


Figure 1-7. Empennage components.

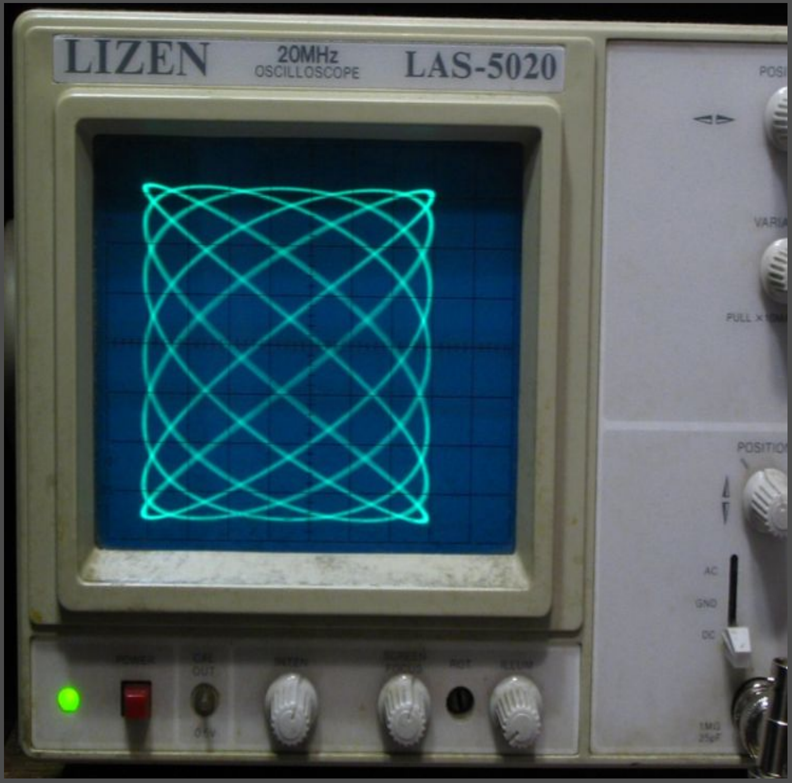
- A small rudder can turn the path of giant ships
- The ship could be just Microsoft, or it can extend to the entire ecosystem
- Is it so crazy to want to unite, like countries of the world fighting an alien invasion?

MSVR Gooooooals!!!



- 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

MSVR Scope



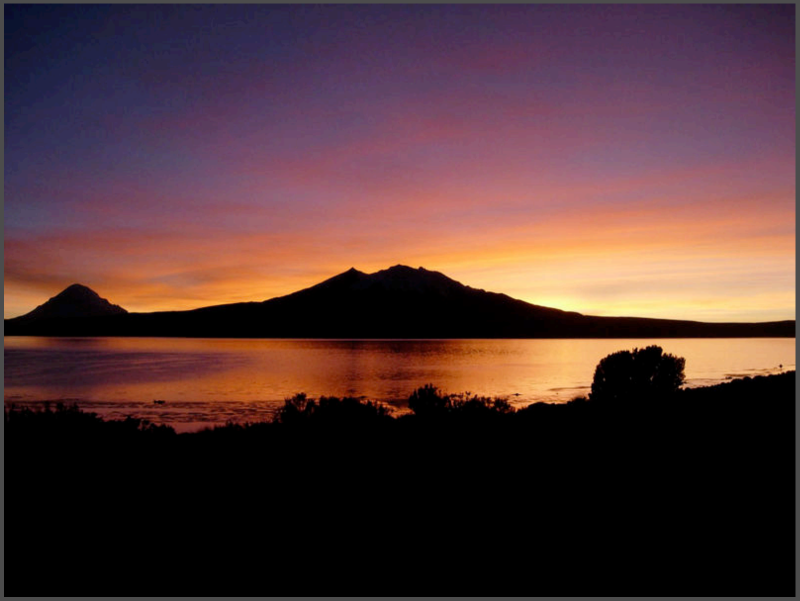
- Begin with 3rd party vendors with the broadest impact to our customers

- 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



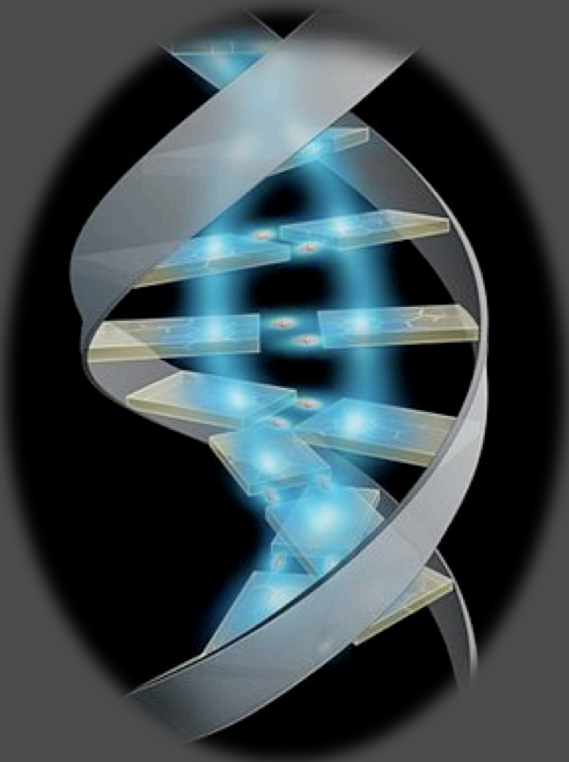
- How will I notice?
  - More secure platform
  - 3rd party vendor acknowledgement
- How can I participate?
  - Try the affected 3rd party vendor first ;-)
  - If you need help, talk to us at msvr@microsoft.com

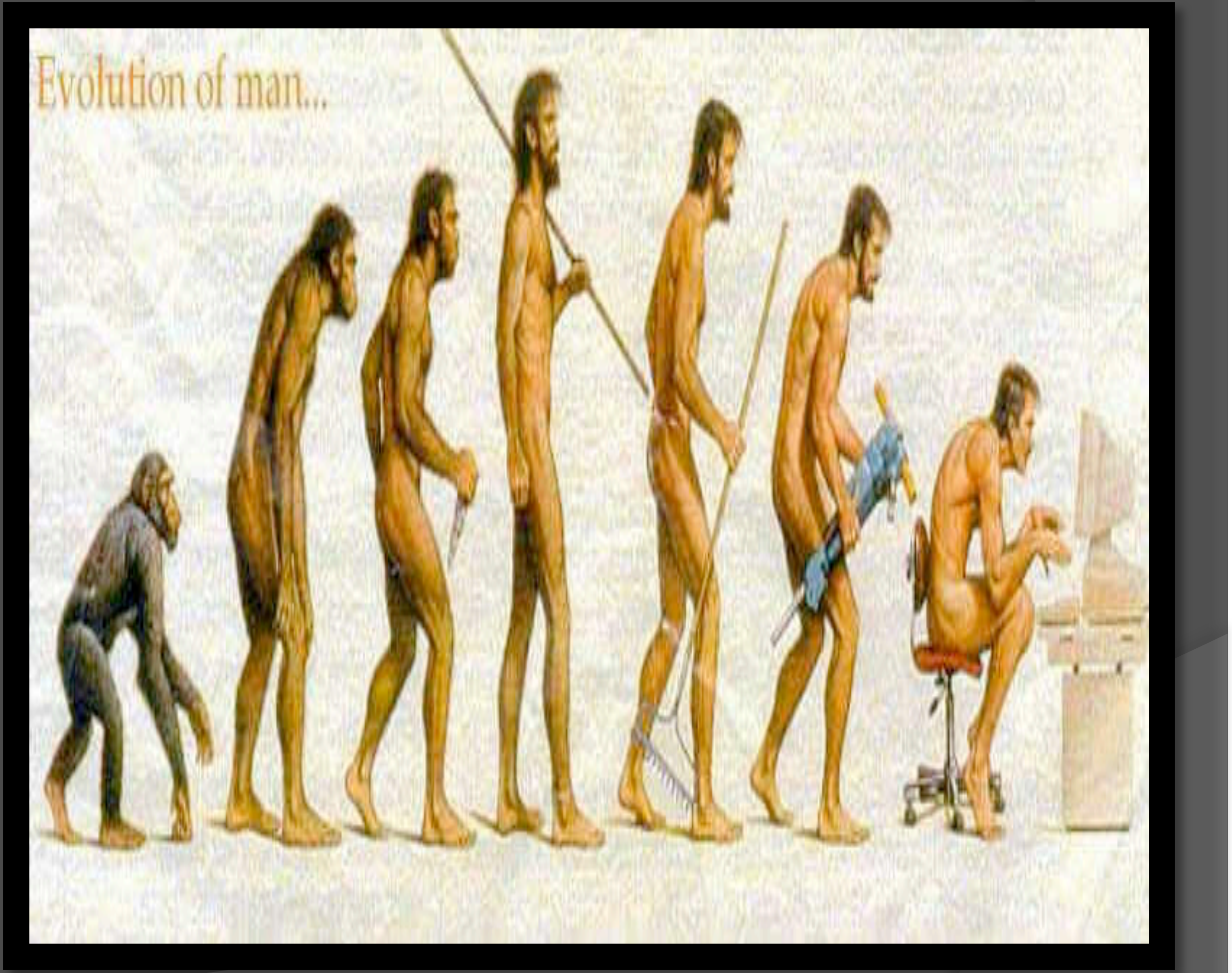
As always, report Microsoft vulnerabilities to us at secure@microsoft.com

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

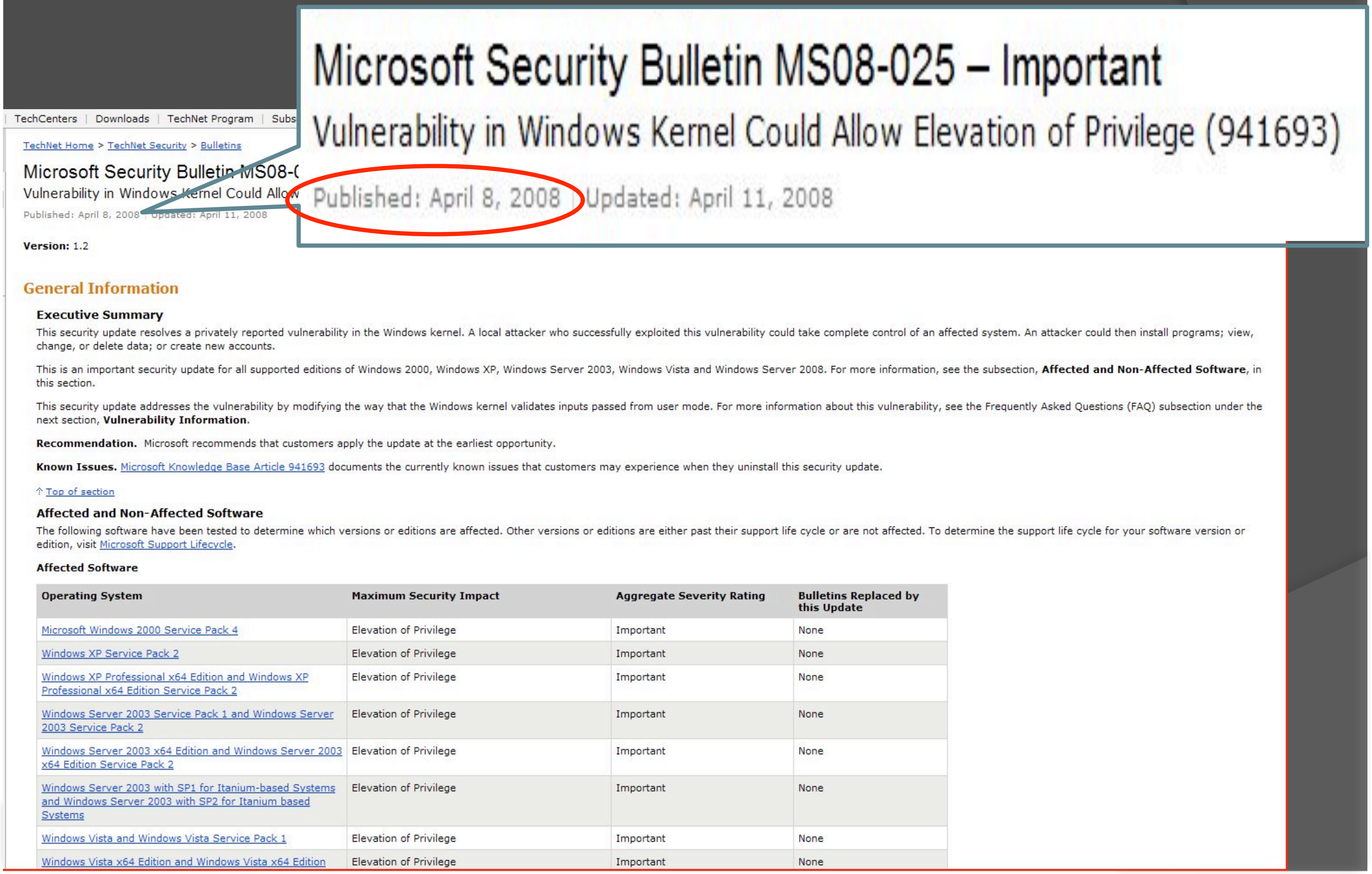
What is the Microsoft Active Protections Program?

- 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

MS08-025 Redux



[TechNet Home](#) > [TechNet Security](#) > [Bulletins](#)

Microsoft Security Bulletin MS08-025 – Important

Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)

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

Microsoft Security Bulletin MS08-(
Vulnerability in Windows Kernel Could Allow
Published: April 8, 2008 | Updated: April 11, 2008

Version: 1.2

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 941693 documents the currently known issues that customers may experience when they uninstall this security update.

↑ Top of section

Affected and Non-Affected Software

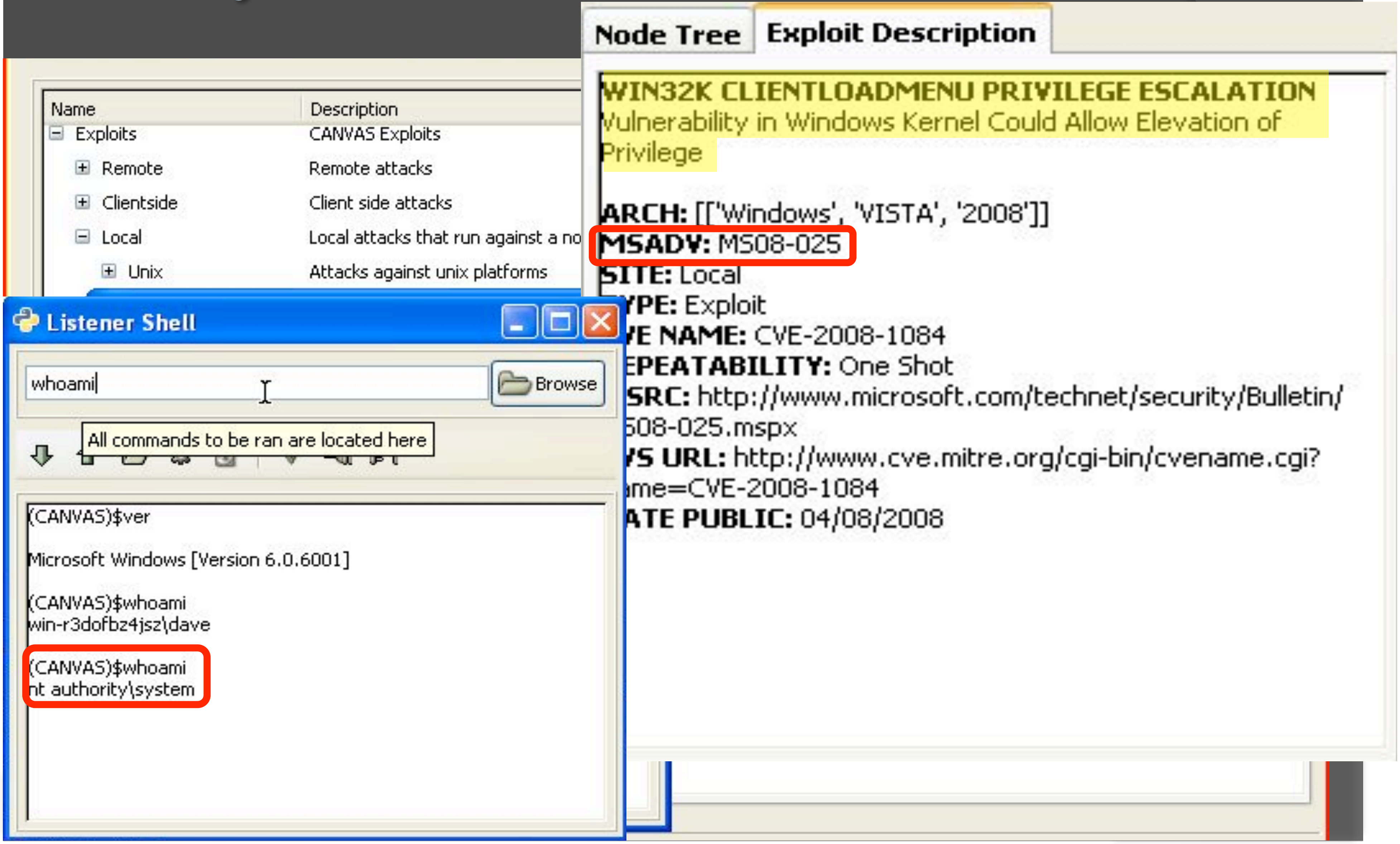
The following software have been tested to determine which versions or editions are affected. Other versions or editions are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, visit Microsoft Support Lifecycle.

Affected Software

Operating System	Maximum Security Impact	Aggregate Severity Rating	Bulletins Replaced by this Update
Microsoft Windows 2000 Service Pack 4	Elevation of Privilege	Important	None
Windows XP Service Pack 2	Elevation of Privilege	Important	None
Windows XP Professional x64 Edition and Windows XP Professional x64 Edition Service Pack 2	Elevation of Privilege	Important	None
Windows Server 2003 Service Pack 1 and Windows Server 2003 Service Pack 2	Elevation of Privilege	Important	None
Windows Server 2003 x64 Edition and Windows Server 2003 x64 Edition Service Pack 2	Elevation of Privilege	Important	None
Windows Server 2003 with SP1 for Itanium-based Systems and Windows Server 2003 with SP2 for Itanium based Systems	Elevation of Privilege	Important	None
Windows Vista and Windows Vista Service Pack 1	Elevation of Privilege	Important	None
Windows Vista x64 Edition and Windows Vista x64 Edition	Elevation of Privilege	Important	None

Can You Say Big Red Button?

So easy a child could do it….



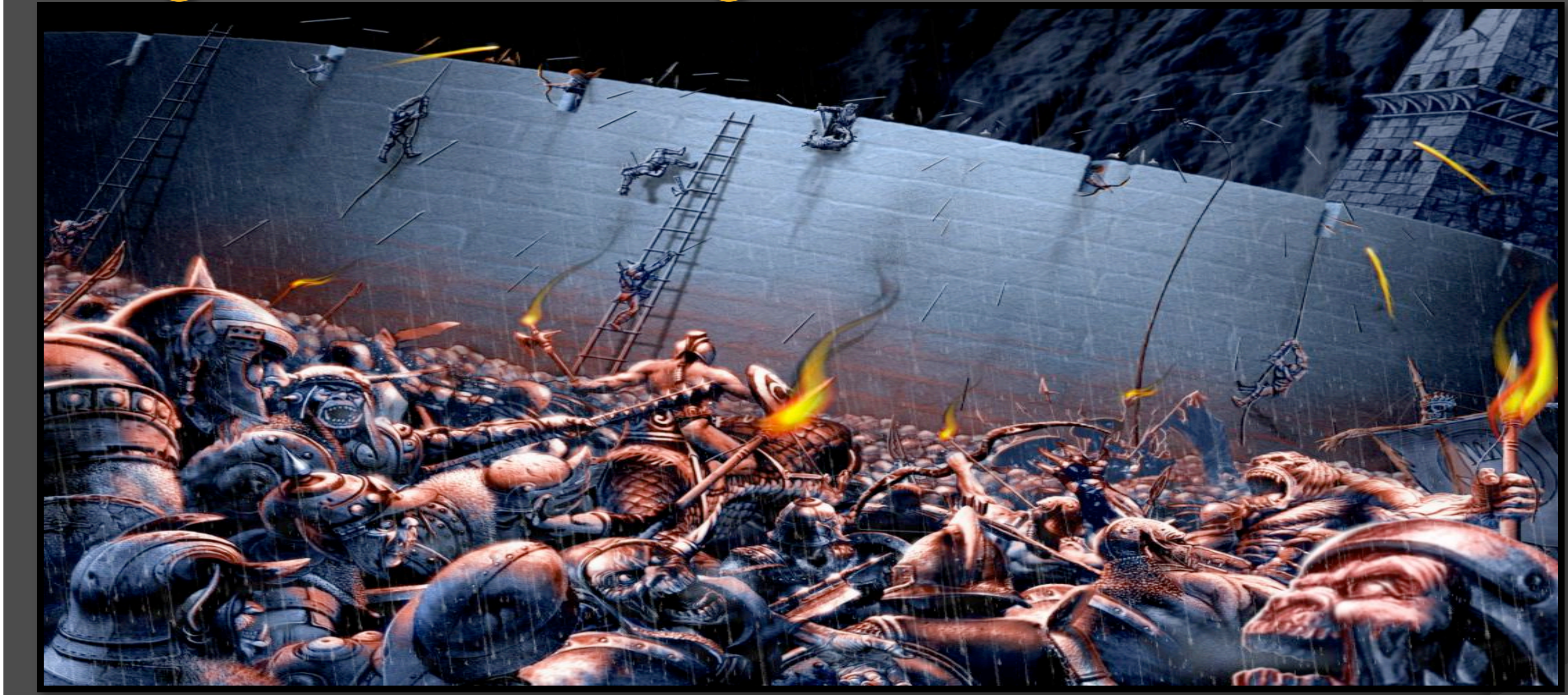
Name	Description
⊟ Exploits	CANVAS Exploits
⊞ Remote	Remote attacks
⊞ Clientside	Client side attacks
⊟ Local	Local attacks that run against a no
⊞ Unix	Attacks against unix platforms

```
(CANVAS)$ver

Microsoft Windows [Version 6.0.6001]

(CANVAS)$whoami
win-r3dofbz4jsz\dave

(CANVAS)$whoami
nt authority\system
```

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

ARCH: [['Windows', 'VISTA', '2008']]
MSADV: MS08-025
SITE: Local
YPE: Exploit
VE NAME: CVE-2008-1084
EPEATABILITY: One Shot
SRC: http://www.microsoft.com/technet/security/Bulletin/
508-025.mspx
VS URL: http://www.cve.mitre.org/cgi-bin/cvename.cgi?
ame=CVE-2008-1084
ATE PUBLIC: 04/08/2008

Age Old Paradigm of Defense



- 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

- To find out more (and to apply)
  - email mapp@microsoft.com

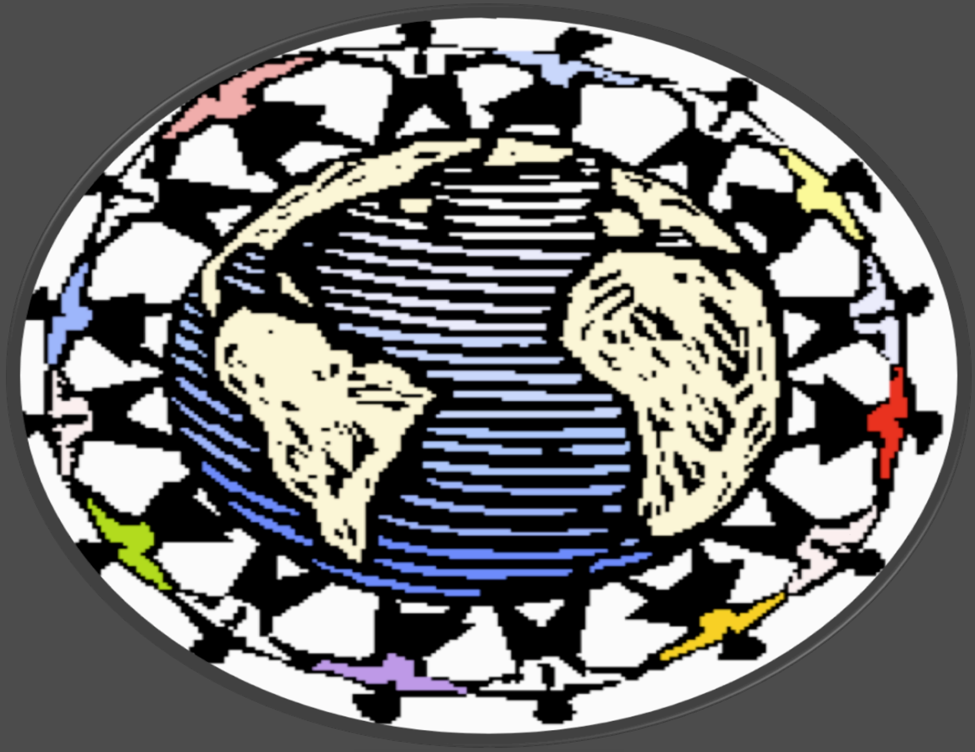
Where are the goods man!...

- Demo of MS08-025

Shout out to Bruce Dang…Go see his talk at 16:45 in Augustus 3/4

demo_GOOD.wmv

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:

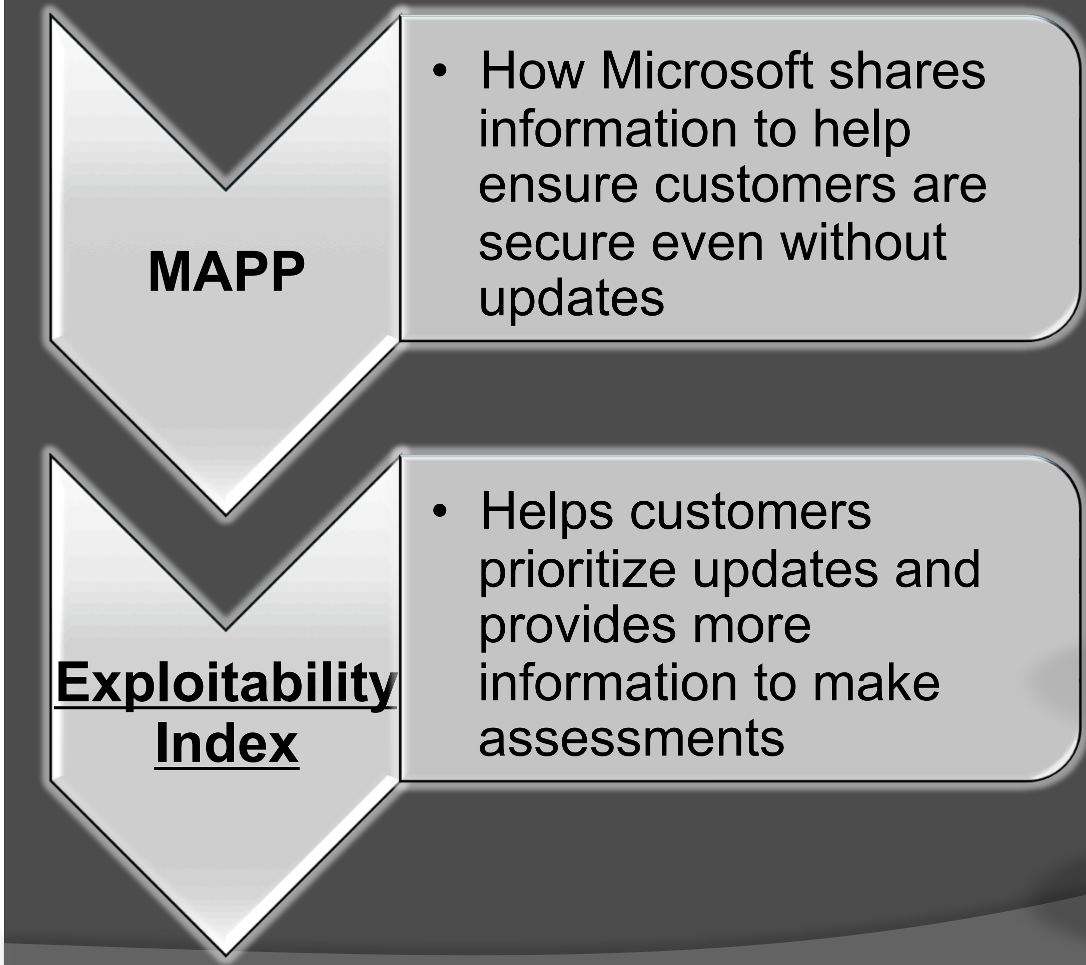
- When's it going to start?
  - October 2008
- Are you worried about someone leaking vulnerability information?
  - The benefits outweigh the risk
  - Safeguard measures have been put in place.
- What if you don't let my favorite product company participate?
  - We are doing everything possible to get 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

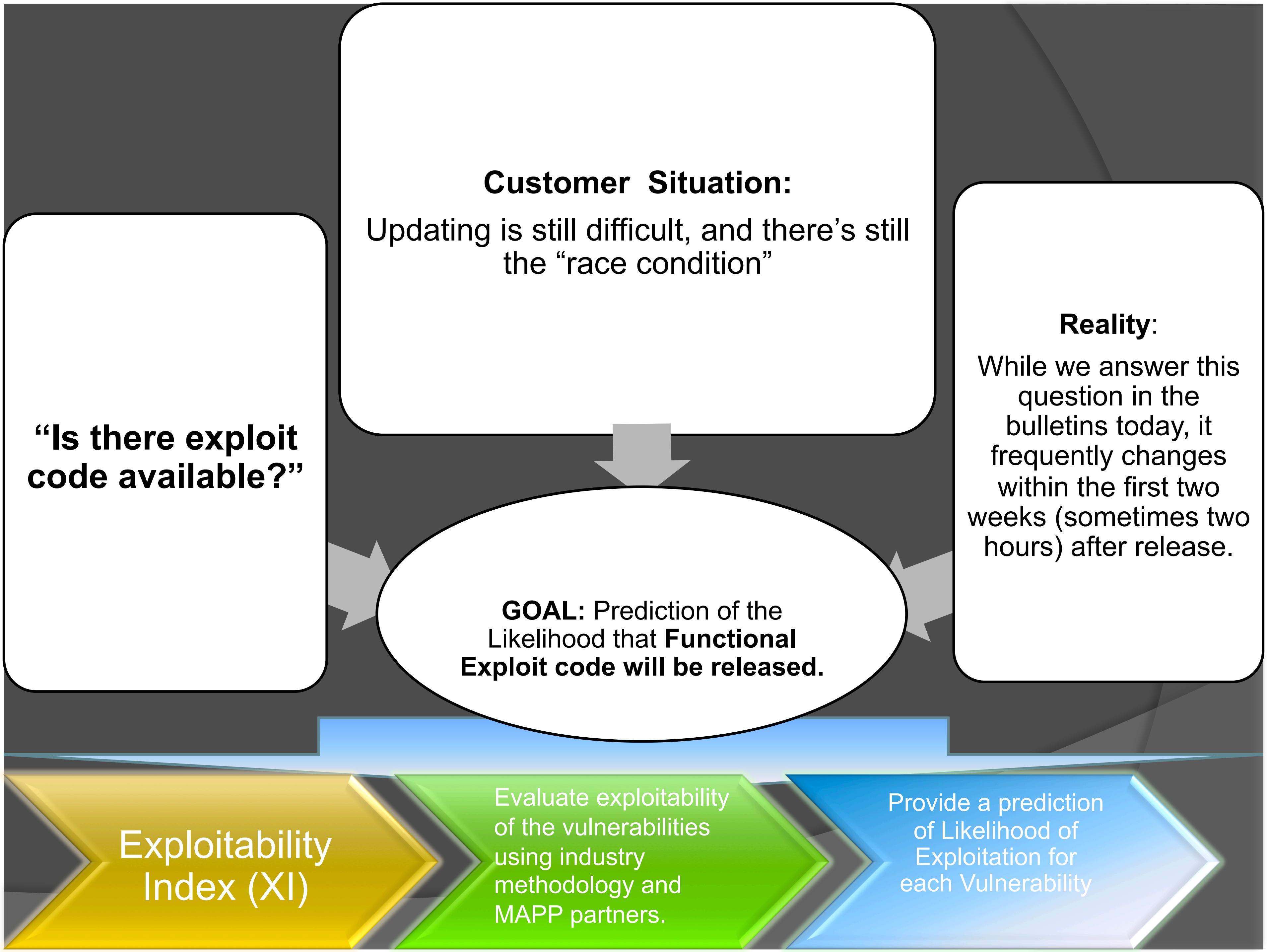
- How Microsoft shares information to help ensure customers are secure even without updates

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”

“Is there exploit code available?”

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.**

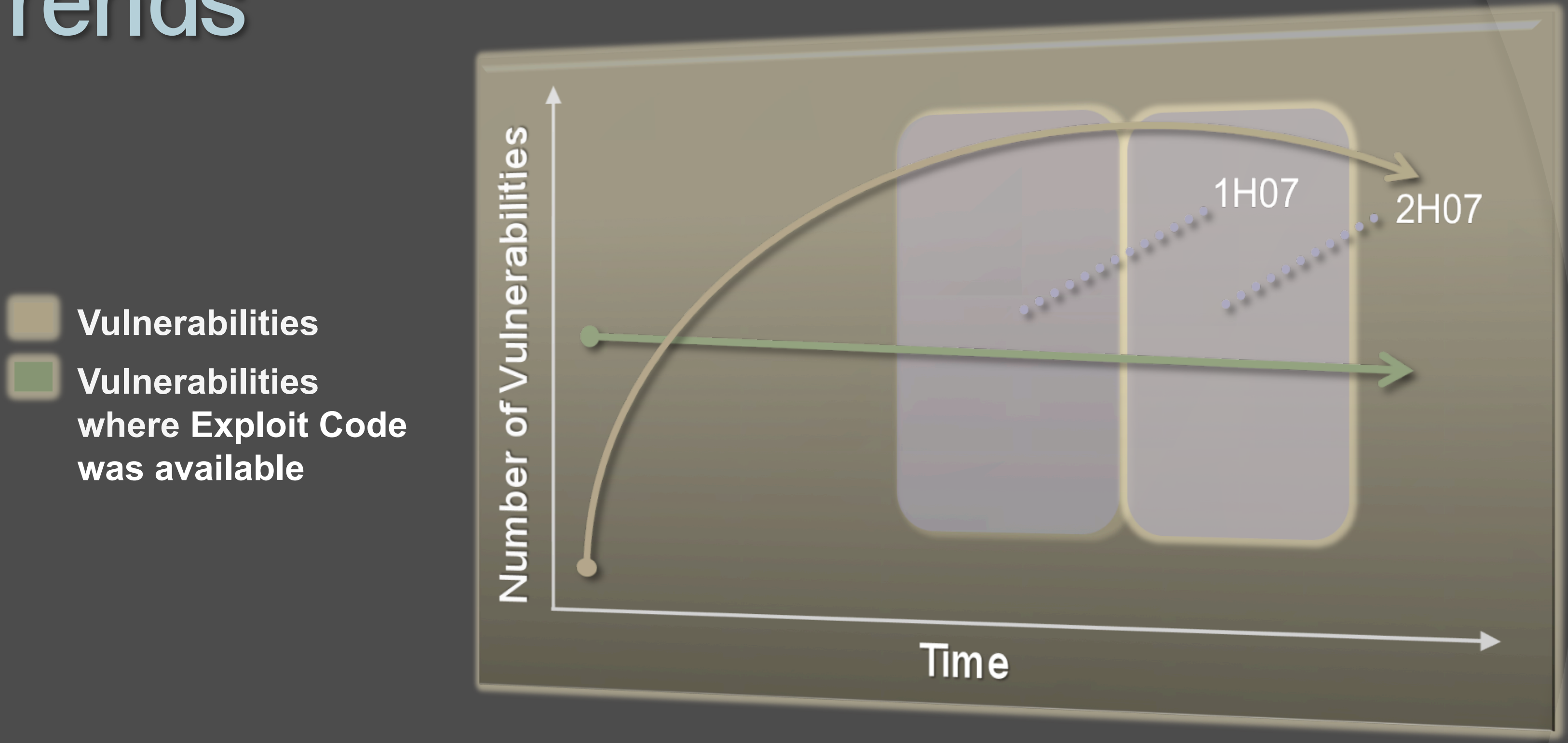
Exploitability Index (XI)

Evaluate exploitability of the vulnerabilities using industry methodology and MAPP partners.

Provide a prediction of Likelihood of Exploitation for each Vulnerability

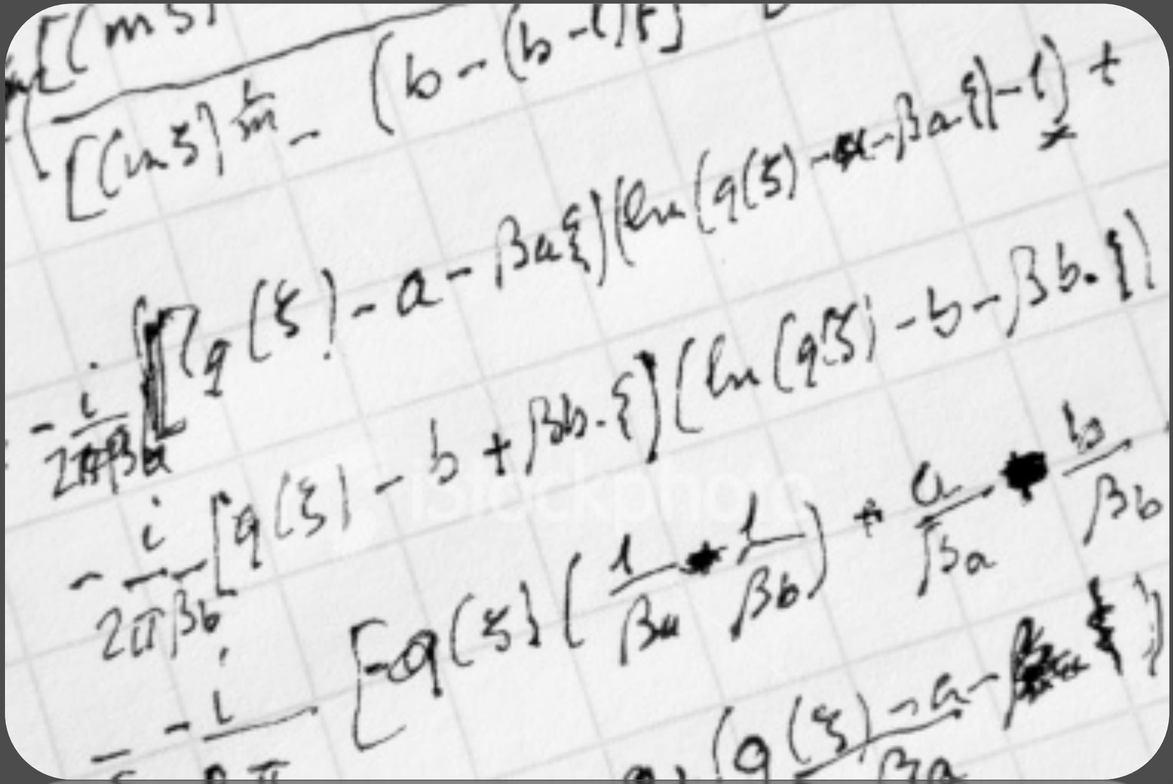
Microsoft Vulnerability Exploit Details

Trends

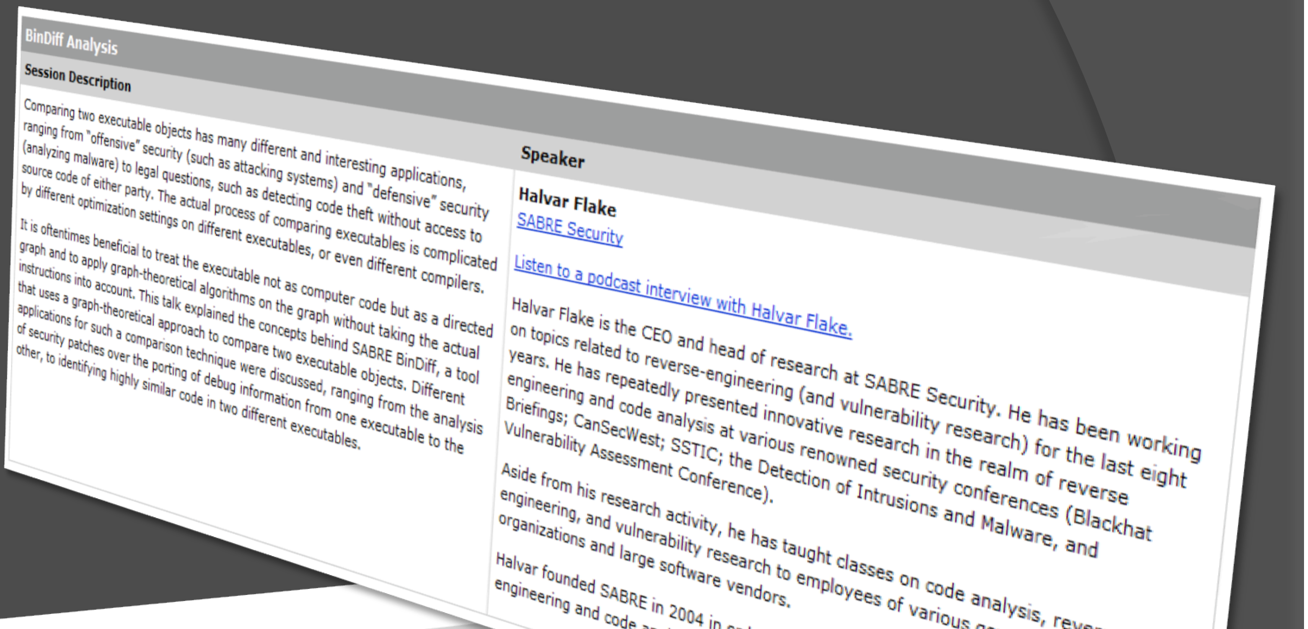


- 2006: 29% of Microsoft vulnerabilities had public exploit code
- 2007: 21% of Microsoft vulnerabilities had public exploit code

How are you making these predicitons?



Listening & Partnering…



BinDiff Analysis

Session Description

Comparing two executable objects has many different and interesting applications, ranging from "offensive" security (such as attacking systems) and "defensive" security (analyzing malware) to legal questions, such as detecting code theft without access to source code of either party. The actual process of comparing executables is complicated by different optimization settings on different executables, or even different compilers.

It is oftentimes beneficial to treat the executable not as computer code but as a directed graph and to apply graph-theoretical algorithms on the graph without taking the actual instructions into account. This talk explained the concepts behind SABRE BinDiff, a tool that uses a graph-theoretical approach to compare two executable objects. Different applications for such a comparison technique were discussed, ranging from the analysis of security patches over the porting of debug information from one executable to the other, to identifying highly similar code in two different executables.

Speaker

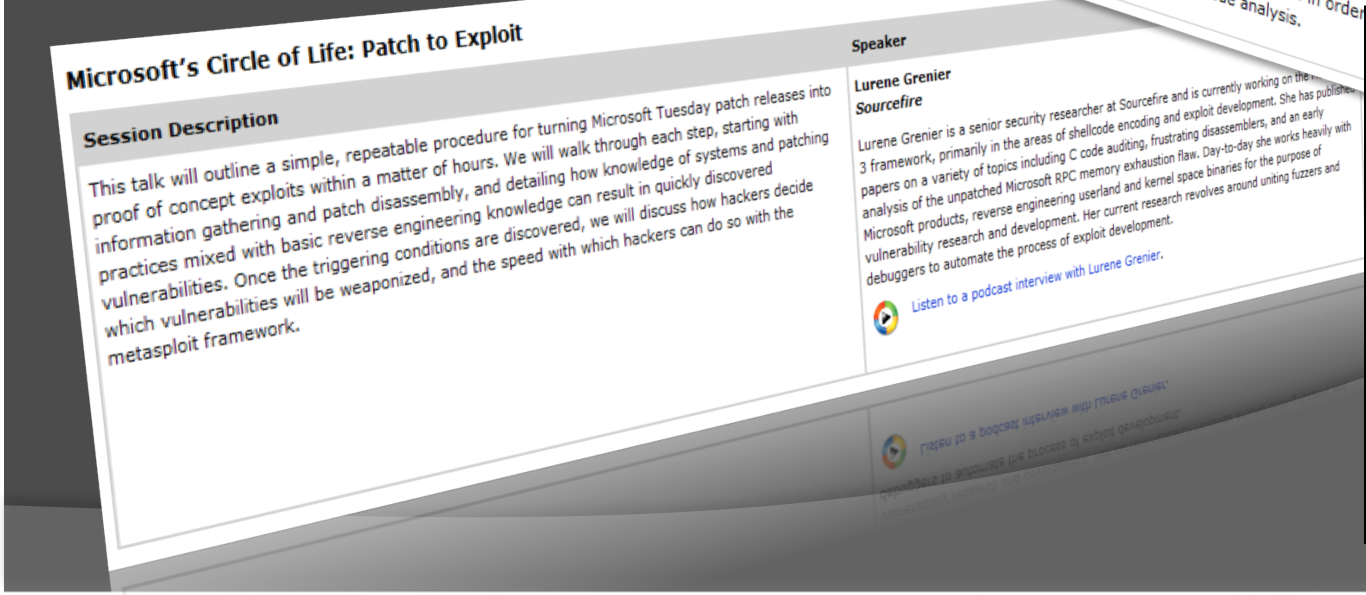
Halvar Flake
SABRE Security

Listen to a podcast interview with Halvar Flake.

Halvar Flake is the CEO and head of research at SABRE Security. He has been working on topics related to reverse-engineering (and vulnerability research) for the last eight years. He has repeatedly presented innovative research in the realm of reverse engineering and code analysis at various renowned security conferences (Blackhat Briefings; CanSecWest; SSTIC; the Detection of Intrusions and Malware, and Vulnerability Assessment Conference).

Aside from his research activity, he has taught classes on code analysis, rever engineering, and vulnerability research to employees of various go organizations and large software vendors.

Halvar founded SABRE in 2004 in order engineering and code analysis.



Microsoft's Circle of Life: Patch to Exploit

Session Description

This talk will outline a simple, repeatable procedure for turning Microsoft Tuesday patch releases into proof of concept exploits within a matter of hours. We will walk through each step, starting with information gathering and patch disassembly, and detailing how knowledge of systems and patching practices mixed with basic reverse engineering knowledge can result in quickly discovered vulnerabilities. Once the triggering conditions are discovered, we will discuss how hackers decide which vulnerabilities will be weaponized, and the speed with which hackers can do so with the metasploit framework.

Speaker

Lurene Grenier
Sourcefire

Lurene Grenier is a senior security researcher at Sourcefire and is currently working on the 3 framework, primarily in the areas of shellcode encoding and exploit development. She has published papers on a variety of topics including C code auditing, frustrating disassemblers, and an early analysis of the unpatched Microsoft RPC memory exhaustion flaw. Day-to-day she works heavily with Microsoft products, reverse engineering userland and kernel space binaries for the purpose of vulnerability research and development. Her current research revolves around uniting fuzzers and debuggers to automate the process of exploit development.

Listen to a podcast interview with Lurene Grenier.

How's it different than…

- Bulletin Severity Ratings
- CVSS

Bulletin Severity Ratings

Critical

- *A vulnerability whose exploitation could allow the propagation of an Internet worm without user action*

Important

- *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*

Moderate

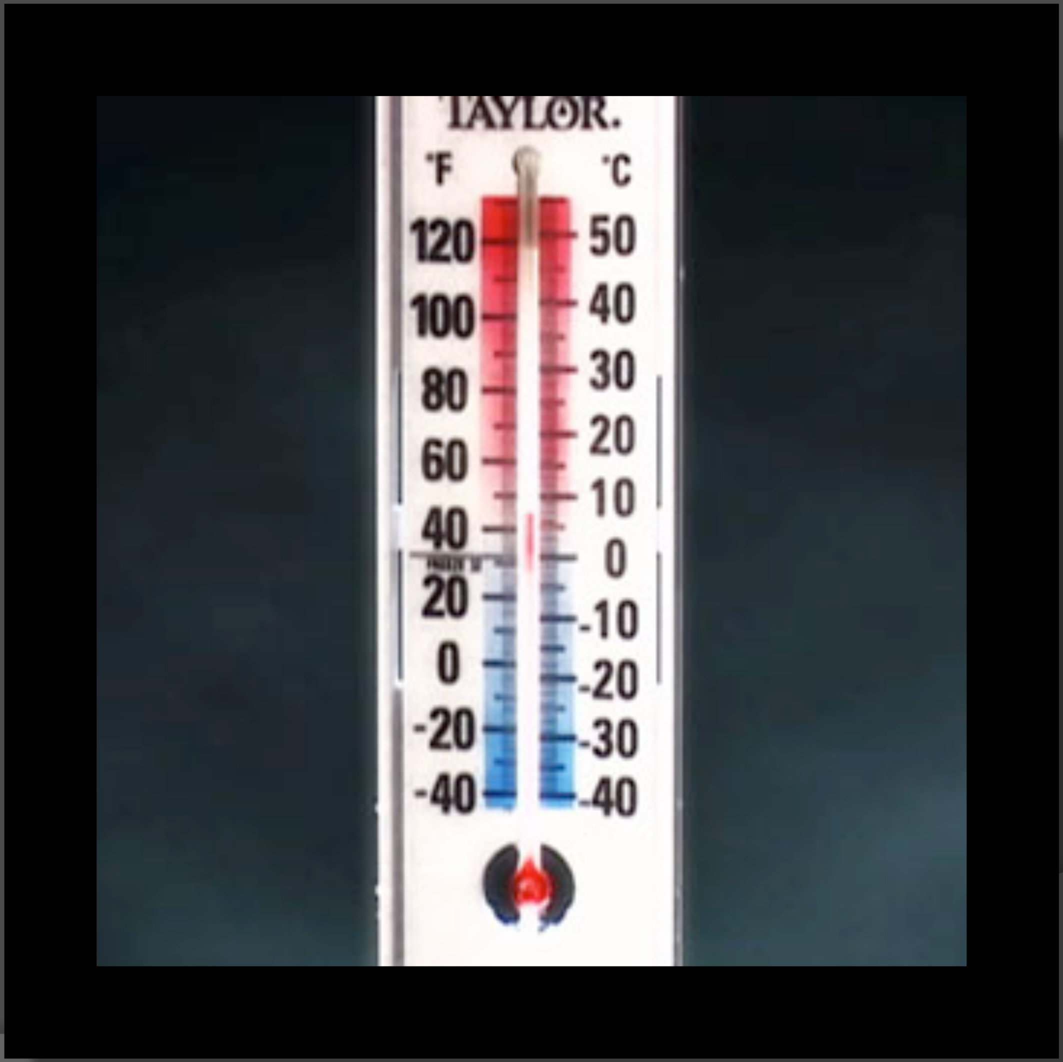
- *Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation*

Low

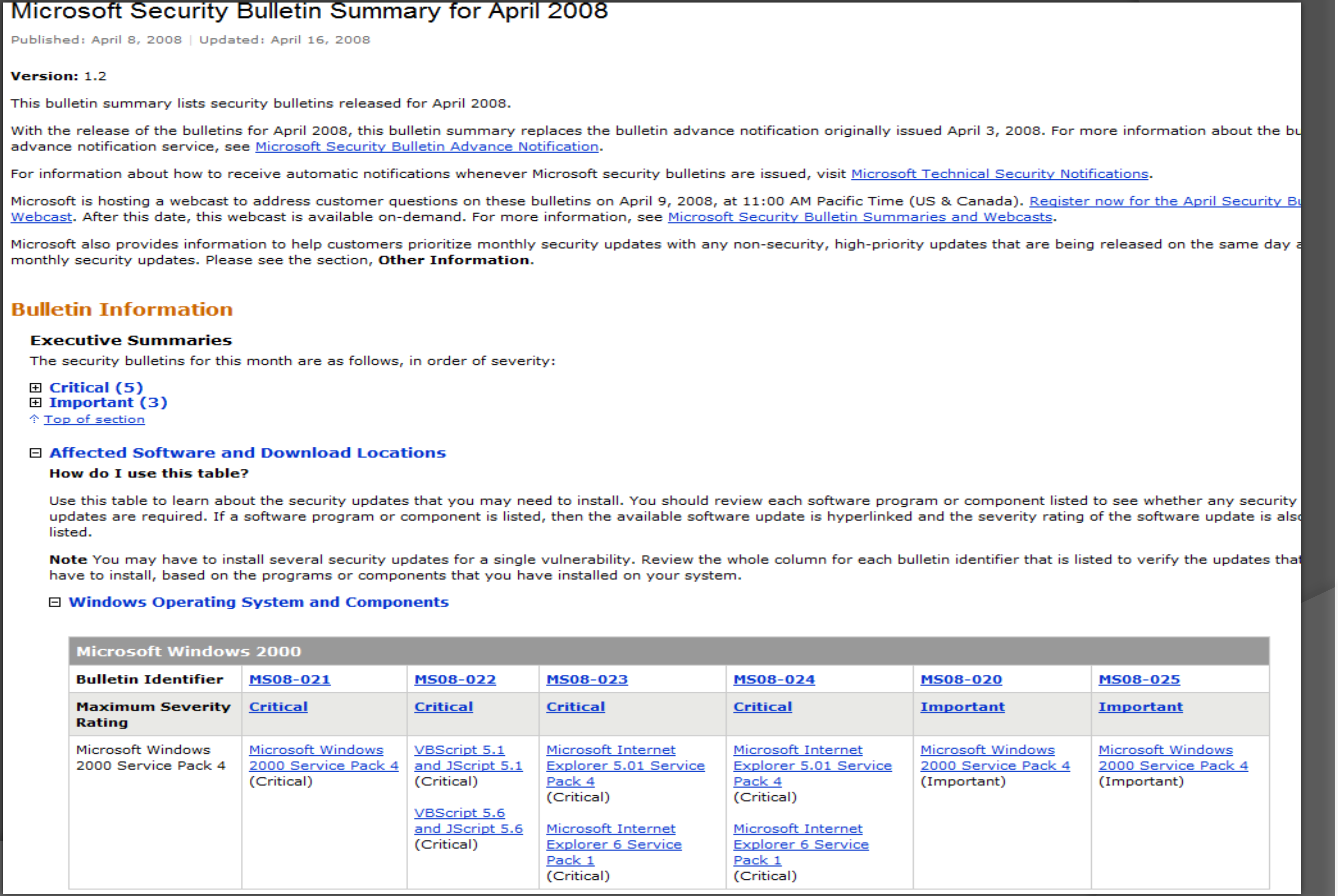
- *A vulnerability whose exploitation is extremely difficult, or whose impact is minimal*

Bulletin Ratings Assume a Determined and Skilled attacker

So what does it look like?



Current Bulletin



Microsoft Security Bulletin Summary for April 2008

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 bu 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 webcast 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 Bu Webcast. After this date, this webcast 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 a 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)**
↑ Top of section

⊟ **Affected Software and Download Locations**

How do I use this table?

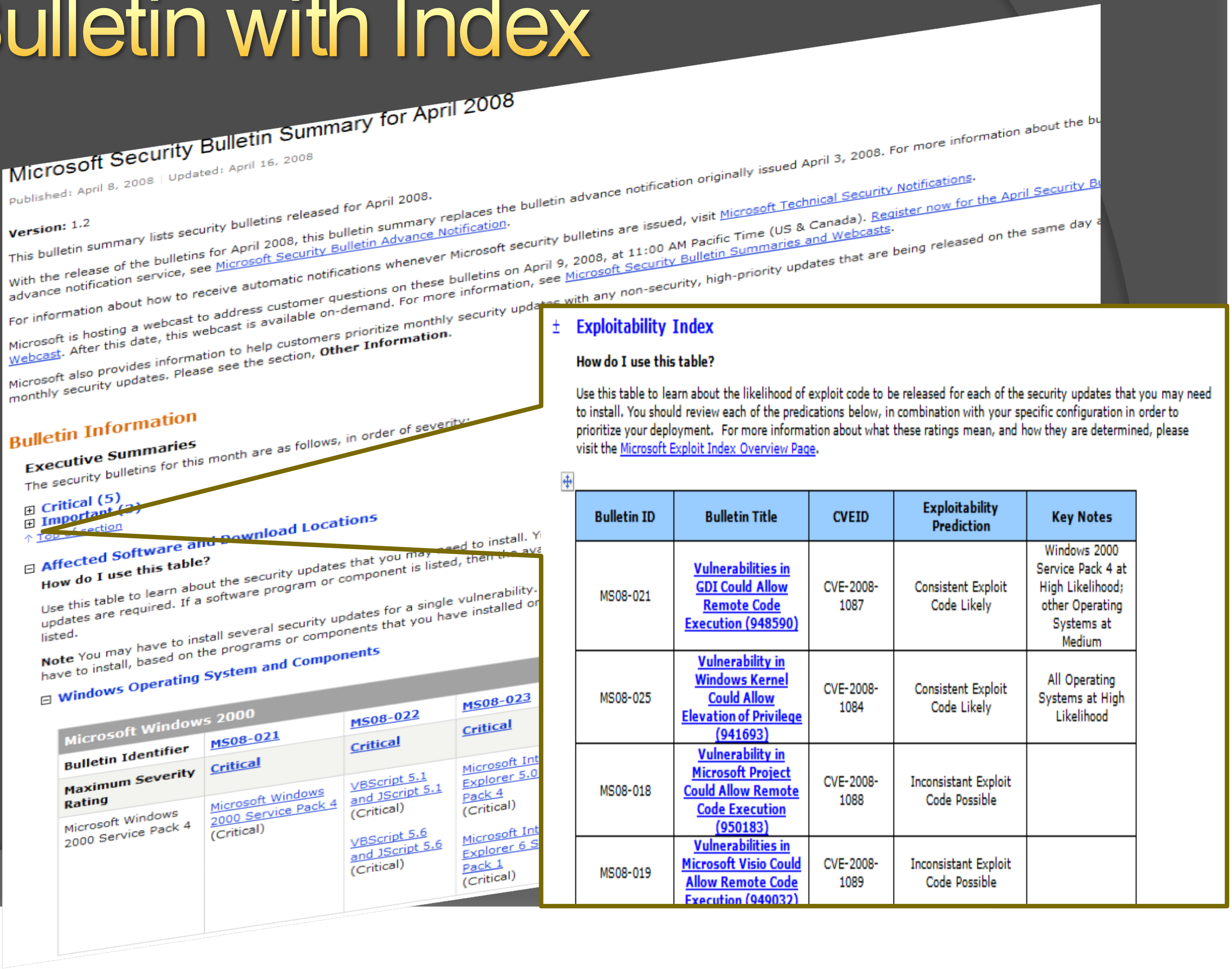
Use this table to learn about the security updates that you may need to install. You should review each software program or component listed to see whether any security updates are required. If a software program or component is listed, then the available software update is hyperlinked and the severity rating of the software update is als 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 tha have to install, based on the programs or components that you have installed on your system.

⊟ **Windows Operating System and Components**

Microsoft Windows 2000						
Bulletin Identifier	**MS08-021**	**MS08-022**	**MS08-023**	**MS08-024**	**MS08-020**	**MS08-025**
Maximum Severity Rating	**Critical**	**Critical**	**Critical**	**Critical**	**Important**	**Important**
Microsoft Windows 2000 Service Pack 4	Microsoft Windows 2000 Service Pack 4 (Critical)	VBScript 5.1 and JScript 5.1 (Critical) VBScript 5.6 and JScript 5.6 (Critical)	Microsoft Internet Explorer 5.01 Service Pack 4 (Critical) Microsoft Internet Explorer 6 Service Pack 1 (Critical)	Microsoft Internet Explorer 5.01 Service Pack 4 (Critical) Microsoft Internet Explorer 6 Service Pack 1 (Critical)	Microsoft Windows 2000 Service Pack 4 (Important)	Microsoft Windows 2000 Service Pack 4 (Important)

Bulletin with Index



Microsoft Security Bulletin Summary for April 2008

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 bu 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 webcast 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 Bu Webcast. After this date, this webcast 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 a 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)
↑ Top of section

⊟ 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. Y updates are required. If a software program or component is listed, then the ava listed.

Note You may have to install several security updates for a single vulnerability. have to install, based on the programs or components that you have installed or

⊟ Windows Operating System and Components

Microsoft Windows 2000			
Bulletin Identifier	MS08-021	MS08-022	MS08-023
Maximum Severity Rating	Critical	Critical	Critical
Microsoft Windows 2000 Service Pack 4	Microsoft Windows 2000 Service Pack 4 (Critical)	VBScript 5.1 and JScript 5.1 (Critical) VBScript 5.6 and JScript 5.6 (Critical)	Microsoft Int Explorer 5.0 Pack 4 (Critical) Microsoft Int Explorer 6 S Pack 1 (Critical)

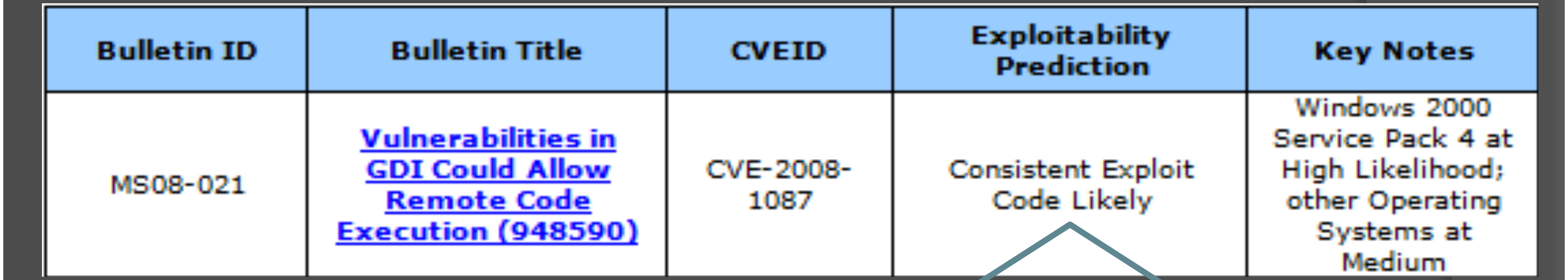
± Exploitability Index

How do I use this table?

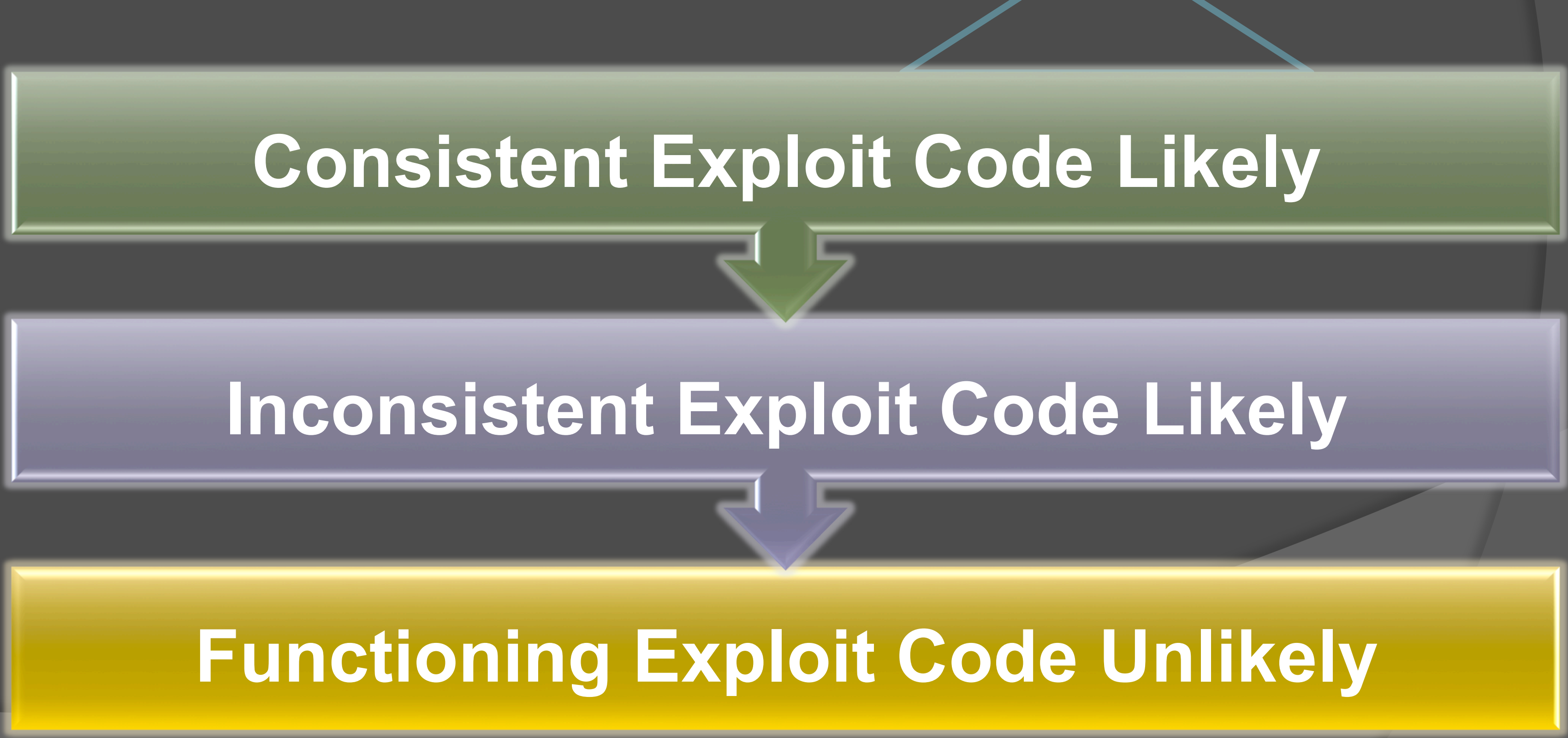
Use this table to learn about the likelihood of exploit code to be released for each of the security updates that you may need to install. You should review each of the predications below, in combination with your specific configuration in order to prioritize your deployment. For more information about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

Bulletin ID	Bulletin Title	CVEID	Exploitability Prediction	Key Notes
MS08-021	Vulnerabilities in GDI Could Allow Remote Code Execution (948590)	CVE-2008-1087	Consistent Exploit Code Likely	Windows 2000 Service Pack 4 at High Likelihood; other Operating Systems at Medium
MS08-025	Vulnerability in Windows Kernel Could Allow Elevation of Privilege (941693)	CVE-2008-1084	Consistent Exploit Code Likely	All Operating Systems at High Likelihood
MS08-018	Vulnerability in Microsoft Project Could Allow Remote Code Execution (950183)	CVE-2008-1088	Inconsistant Exploit Code Possible	
MS08-019	Vulnerabilities in Microsoft Visio Could Allow Remote Code Execution (949032)	CVE-2008-1089	Inconsistant Exploit Code Possible	

Understanding the Index



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



Consistent Exploit Code Likely

Inconsistent Exploit Code Likely

Functioning Exploit Code Unlikely

Track Record – Last 5 Mos.

Bulletin Number	Bulletin Name	Release Date	CVE	Severity	Exploitability Prediction	Accuracy
MS08-030	Bluetooth	6/10/2008	CVE-2008-1453	Critical	Inconsistent Exploit Code Likely	Correct
MS08-022	Script	4/8/2008	CVE-2008-0083	Critical	Inconsistent Exploit Code Likely	Correct
MS08-032	ActiveX	6/10/2008	CVE-2007-0675		Functioning Exploit Code Unlikely	Correct
MS08-037	DNS	7/8/2008	CVE-2008-1447	Important	Consistent Exploit Code Likely	Correct
MS08-031	Internet Explorer	6/10/2008	CVE-2008-1544	Important	Consistent Exploit Code Likely	Correct
MS08-031	Internet Explorer	6/10/2008	CVE-2008-1442	Critical	Consistent Exploit Code Likely	Correct
MS08-033	DirectX	6/10/2008	CVE-2008-0011	Critical	Consistent Exploit Code Likely	Correct
MS08-033	WMP	6/10/2008	CVE-2008-1444	Critical	Consistent Exploit Code Likely	Correct
MS08-021	GDI32	4/8/2008	CVE-2008-1087	Critical	Consistent Exploit Code Likely	Correct
MS08-025	Win32	4/8/2008	CVE-2008-1084	Important	Consistent Exploit Code Likely	Correct
MS08-015	Outlook	3/11/2008	CVE-2008-0110	Critical	Consistent Exploit Code Likely	Correct
MS08-017	OWC	3/11/2008	CVE-2007-1201	Critical	Consistent Exploit Code Likely	Correct
MS08-017	OWC	3/11/2008	CVE-2006-4695	Critical	Consistent Exploit Code Likely	Correct
MS08-019	Visio	4/8/2008	CVE-2008-1090	Important	Inconsistent Exploit Code Likely	N/A
MS08-037	DNS	7/8/2008	CVE-2008-1454	Important	Inconsistent Exploit Code Likely	None Posted
MS08-038	Explorer	7/8/2008	CVE-2008-1435	Important	Inconsistent Exploit Code Likely	None Posted
MS08-040	SQL Page Reuse	7/8/2008	CVE-2008-0085	Important	Inconsistent Exploit Code Likely	None Posted
MS08-040	SQL MemCorruption	7/8/2008	CVE-2008-0107	Important	Inconsistent Exploit Code Likely	None Posted
MS08-034	WINS	6/10/2008	CVE-2008-1451	Important	Inconsistent Exploit Code Likely	None Posted
MS08-026	Word	5/13/2008	CVE-2008-1434	Critical	Inconsistent Exploit Code Likely	None Posted
MS08-027	Publisher	5/13/2008	CVE-2008-0119	Critical	Inconsistent Exploit Code Likely	None Posted
MS08-020	DNS	4/8/2008	CVE-2008-0087	Important	Inconsistent Exploit Code Likely	None Posted
MS08-021	GDI32	4/8/2008	CVE-2008-1083	Critical	Inconsistent Exploit Code Likely	None Posted
MS08-023	Killbit	4/8/2008	CVE-2008-1086	Critical	Inconsistent Exploit Code Likely	None Posted
MS08-024	IE	4/8/2008	CVE-2008-1085	Critical	Inconsistent Exploit Code Likely	None Posted
MS08-014	Excel	3/11/2008	CVE-2008-0112	Important	Inconsistent Exploit Code Likely	None Posted
MS08-035	NTDSA DoS	6/10/2008	CVE-2008-1445	Important	Functioning Exploit Code Unlikely	None Posted
MS08-036	PGM DoS	6/10/2008	CVE-2008-1440	Important	Functioning Exploit Code Unlikely	None Posted
MS08-036	PGM DoS	6/10/2008	CVE-2008-1441	Important	Functioning Exploit Code Unlikely	None Posted
MS08-026	Word	5/13/2008	CVE-2008-1091	Critical	Functioning Exploit Code Unlikely	None Posted
MS08-014	Excel	3/11/2008	CVE-2008-0114	Critical	Functioning Exploit Code Unlikely	None Posted
MS08-039	OWA	7/8/2008	CVE-2008-2247	Important	Consistent Exploit Code Likely	None Posted
MS08-039	OWA	7/8/2008	CVE-2008-2248	Important	Consistent Exploit Code Likely	None Posted
MS08-040	SQL BO	7/8/2008	CVE-2008-0086	Important	Consistent Exploit Code Likely	None Posted
MS08-040	SQL BO	7/8/2008	CVE-2008-0106	Important	Consistent Exploit Code Likely	None Posted
MS08-014	Excel	3/11/2008	CVE-2008-0111	Critical	Consistent Exploit Code Likely	None Posted
MS08-014	Excel	3/11/2008	CVE-2008-0081	Critical	Consistent Exploit Code Likely	None Posted
MS08-019	Visio	4/8/2008	CVE-2008-1089	Important	Not Analyzed	N/A
MS08-029	Malware Engine	5/13/2008	CVE-2008-1437	Important	Not Analyzed	N/A
MS08-029	Malware Engine	5/13/2008	CVE-2008-1438	Important	Not Analyzed	N/A
MS08-018	Project	4/8/2008	CVE-2008-1088	Critical	Not Analyzed	N/A
MS08-014	Excel	3/11/2008	CVE-2008-0116	Critical	Not Analyzed	N/A
MS08-014	Excel	3/11/2008	CVE-2008-0117	Critical	Not Analyzed	N/A
MS08-014	Excel	3/11/2008	CVE-2008-0115	Critical	Not Analyzed	N/A
MS08-016	Office	3/11/2008	CVE-2008-0113	Critical	Not Analyzed	N/A
MS08-016	Office	3/11/2008	CVE-2008-0118	Critical	Not Analyzed	N/A
MS08-028	Word and Access	5/13/2008	CVE-2007-6026	Important	Public At Release	N/A

"Consistent Exploit Likely"

-Applies to 16/37 CVEs

-57% reduction.

"Consistent & Inconsistent Exploit Likely"

-Applies to 31/37

-16% reduction

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
  - http://blogs.technet.com/**ecostrat**/

Q&A