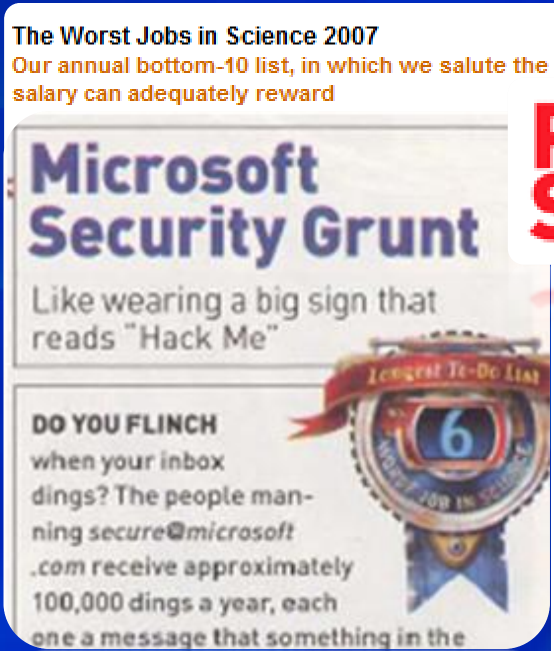
# *Behind the curtain*
# Microsoft Vulnerability Response Explained

Mike Reavey
Director
Microsoft Security Response Center
Microsoft Corporation

# Agenda

- Overall Vulnerability Remediation Process
- Ecosystem Focus
- Emergency Response – “SSIRP”

# Awards!



The Worst Jobs in Science 2007

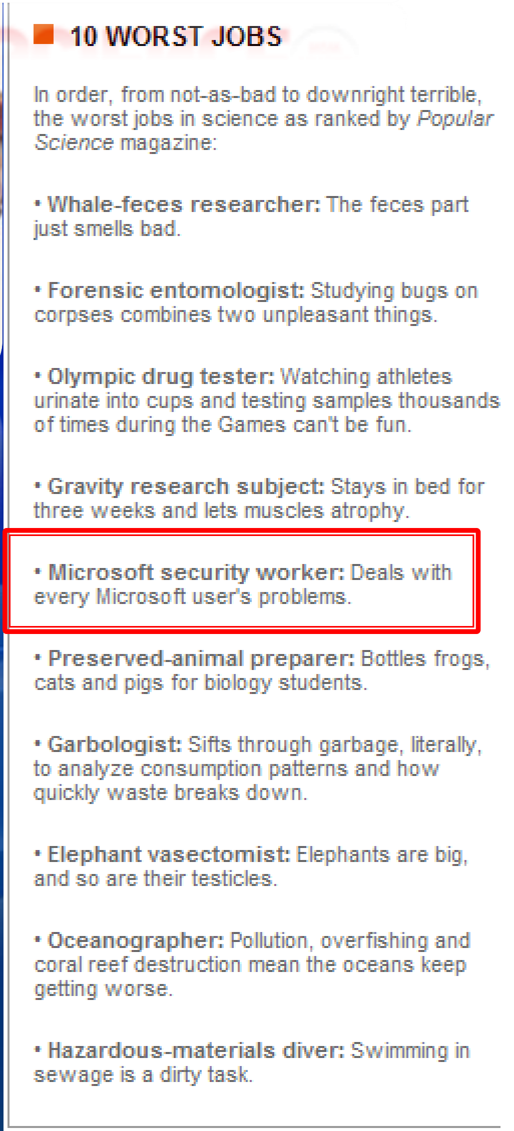
Our annual bottom-10 list, in which we salute the men and women who do what no salary can adequately reward

POPULAR SCIENCE

## Microsoft Security Grunt

Like wearing a big sign that reads "Hack Me"

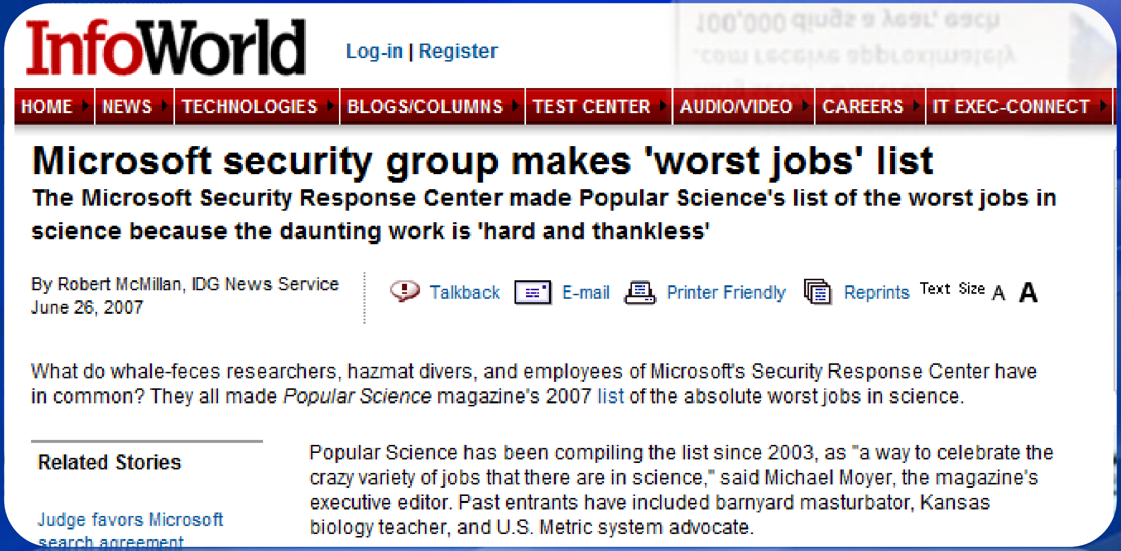
**DO YOU FLINCH** when your inbox dings? The people manning *secure@microsoft.com* receive approximately 100,000 dings a year, each one a message that something in the



**10 WORST JOBS**

In order, from not-as-bad to downright terrible, the worst jobs in science as ranked by *Popular Science* magazine:

- **Whale-feces researcher:** The feces part just smells bad.
- **Forensic entomologist:** Studying bugs on corpses combines two unpleasant things.
- **Olympic drug tester:** Watching athletes urinate into cups and testing samples thousands of times during the Games can't be fun.
- **Gravity research subject:** Stays in bed for three weeks and lets muscles atrophy.
- **Microsoft security worker:** Deals with every Microsoft user's problems.
- **Preserved-animal preparer:** Bottles frogs, cats and pigs for biology students.
- **Garbologist:** Sifts through garbage, literally, to analyze consumption patterns and how quickly waste breaks down.
- **Elephant vasectomist:** Elephants are big, and so are their testicles.
- **Oceanographer:** Pollution, overfishing and coral reef destruction mean the oceans keep getting worse.
- **Hazardous-materials diver:** Swimming in sewage is a dirty task.



InfoWorld Log-in | Register

## Microsoft security group makes 'worst jobs' list

**The Microsoft Security Response Center made Popular Science's list of the worst jobs in science because the daunting work is 'hard and thankless'**

By Robert McMillan, IDG News Service
June 26, 2007

What do whale-feces researchers, hazmat divers, and employees of Microsoft's Security Response Center have in common? They all made *Popular Science* magazine's 2007 list of the absolute worst jobs in science.

**Related Stories**

Judge favors Microsoft search agreement

Popular Science has been compiling the list since 2003, as "a way to celebrate the crazy variety of jobs that there are in science," said Michael Moyer, the magazine's executive editor. Past entrants have included barnyard masturbator, Kansas biology teacher, and U.S. Metric system advocate.

# Microsoft Security Response Center

**Investigate and Resolve Vulnerability Reports**

- Staff public reporting alias
- Monitor security lists
- Single point of coordination and communications

**Microsoft Security Response Process**

- Own and coordinate company wide process
- Work to prevent issues through security engineering and development process changes

**Building Relationships and Communications**

- Work with law enforcement and industry influentials
- Create community with vulnerability finders

# MSRC Focus Areas

- Protect our customers
- Live up to the Security Promise made to customers
- Preserve customer confidence in MS products
- Provide Risk Management - Analyzing threats and guide a response to them
- Understand the security ecosystem
- Work with partners as part of distributed defense network
- Root cause analysis and provide feedback and guidance to product groups (SDL)

# Building a Security Response Process

## Security Bulletin Release Process

Build a more Simplified, Manageable Process

Enhance and Improve Bulletin Content

Expand Resources and Support

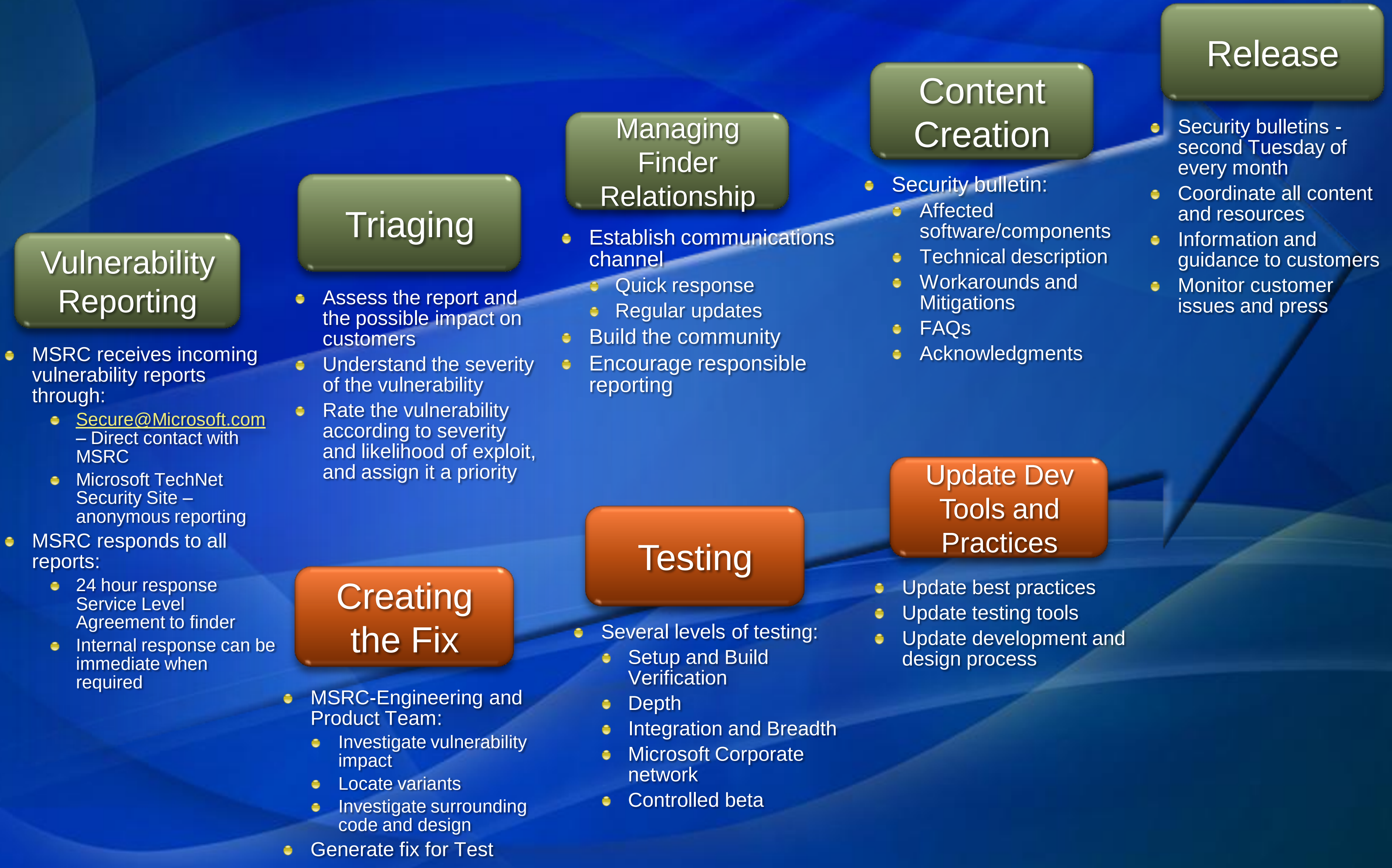
## Security Incident Response Process

Provide Timely and Relevant Information

Help Mitigate and Protect

Deliver Solution to Resolve

# Releasing a Security Update



## Vulnerability Reporting

- MSRC receives incoming vulnerability reports through:
  - Secure@Microsoft.com – Direct contact with MSRC
  - Microsoft TechNet Security Site – anonymous reporting
- MSRC responds to all reports:
  - 24 hour response Service Level Agreement to finder
  - Internal response can be immediate when required

## Triaging

- Assess the report and the possible impact on customers
- Understand the severity of the vulnerability
- Rate the vulnerability according to severity and likelihood of exploit, and assign it a priority

## Creating the Fix

- MSRC-Engineering and Product Team:
  - Investigate vulnerability impact
  - Locate variants
  - Investigate surrounding code and design
- Generate fix for Test

## Managing Finder Relationship

- Establish communications channel
  - Quick response
  - Regular updates
- Build the community
- Encourage responsible reporting

## Testing

- Several levels of testing:
  - Setup and Build Verification
  - Depth
  - Integration and Breadth
  - Microsoft Corporate network
  - Controlled beta

## Content Creation

- Security bulletin:
  - Affected software/components
  - Technical description
  - Workarounds and Mitigations
  - FAQs
  - Acknowledgments

## Update Dev Tools and Practices

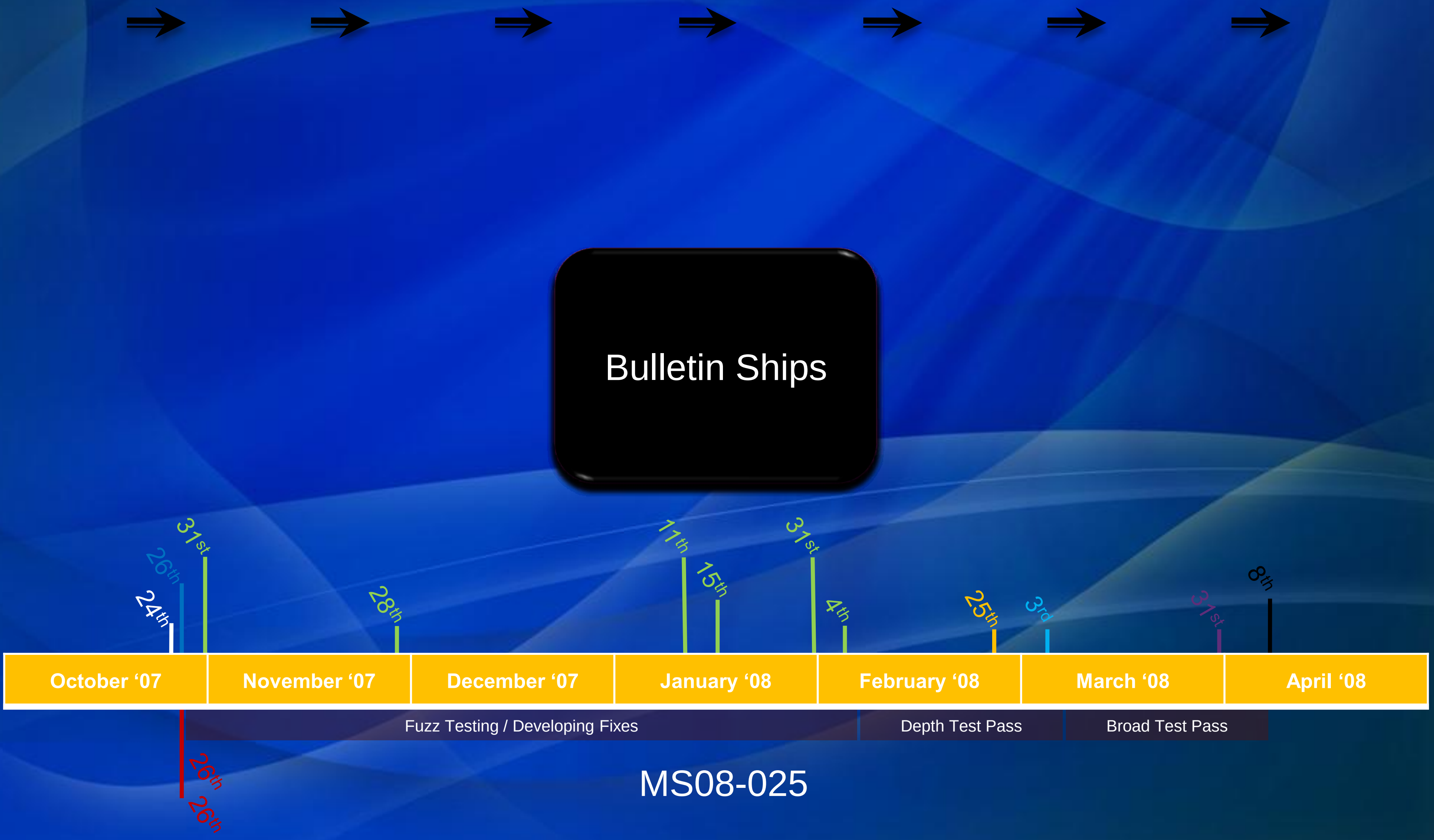
- Update best practices
- Update testing tools
- Update development and design process

## Release

- Security bulletins - second Tuesday of every month
- Coordinate all content and resources
- Information and guidance to customers
- Monitor customer issues and press

Microsoft Confidential

# Internal Process



Bulletin Ships

Fuzz Testing / Developing Fixes

Depth Test Pass

Broad Test Pass

MS08-025

# MSRC Ecosystem Strategy Team

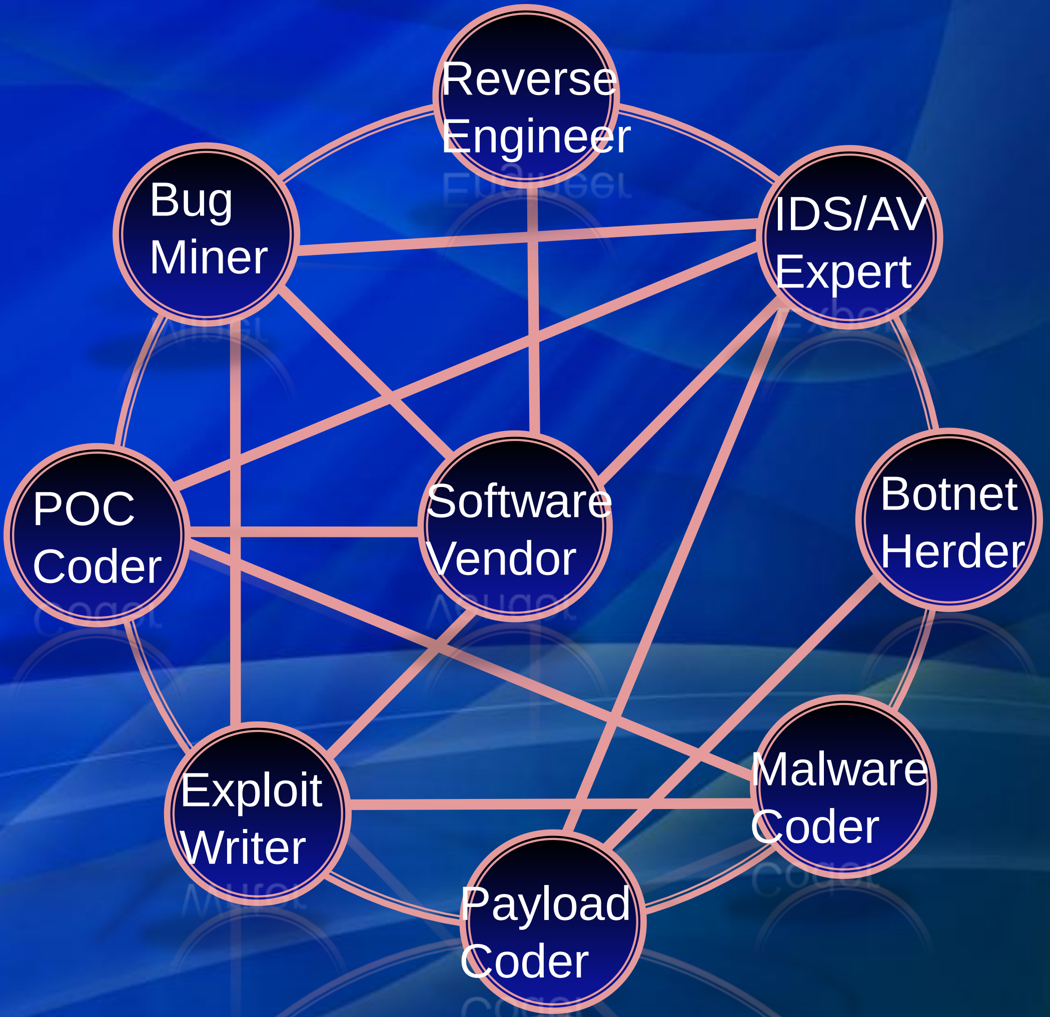
- One of many outreach teams at MS, includes hacker, partner, CERT outreach
- Understand security issues at the intersection of technology and the human element
- Focus on understanding and expanding trust networks inside and outside of M$
- Provide a positive outlet for researcher creativity as a formalized evolution of our response / engineering capabilities

# EcoStrat Focus Areas

- Protect our customers
- Live up to the Security Promise made to customers
- Preserve customer confidence in MS products
- Provide Risk Management - Analyzing threats and guide a response to them
- Understand the security ecosystem
- Work with partners as part of distributed defense network
- Root cause analysis and provide feedback and guidance to product groups (SDL)

# EcoStrat Activities

- Actors
  - Understand decision making process - Engage all segments in community-based defense
- Technology
  - Identify attack & research trends - Extinguish classes of issues
- Economics
  - Promote legitimate business opportunities
  - Increase the cost of illegal activities



# Security Ecosystem: Opportunities & Strategy

- Primarily influencing researchers and community and indirectly changing the ecosystem

- Where
  - Home (Microsoft Campus)
  - There (conferences, external visits, their watering holes)
  - Everywhere (communication through networks)

- How
  - 1:1
  - 1:Many
  - Many:Many

# Security Ecosystem Trends

- Increased Number of Reported Vulnerabilities
  - Industry – wide problem
- Increased Number of Affected Products
  - Attacks targeting 3rd party applications & drivers
- Specialization and Tools:
  - Specialists – Vulnerabilities Miners, Exploit Writers
  - Sophisticated Tools
- Increasing Velocity:
  - The Time from patch to exploit is shrinking
- Money Economy
  - Widespread Malicious Attacks
  - Isolated & Targeted Attacks

# Ecosystem Evolution

- Escalation of Attacks & Intensity of Attacker Focus
  - Many different motivations
  - Many different origins
- Securing customers requires a new paradigm
  - New partnerships and strategies needed
- Microsoft to drive Community Based Defense
  - Extend MSRC Response Process and Methods
  - SDL & Security Engineering for other ISVs
  - Defense in Depth and Security Education critical

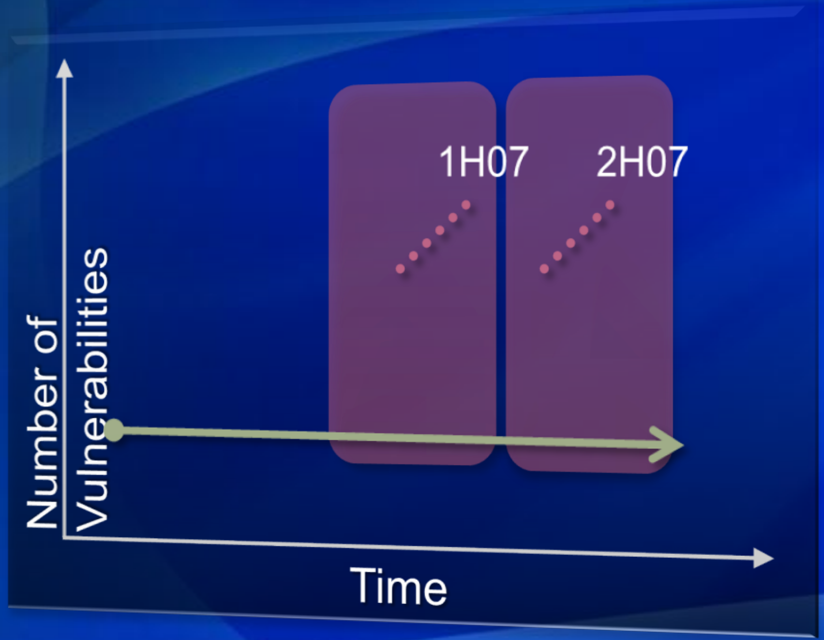
# What can we do?

- Community-Based Defense.
- Continue building strategic durable relationships and alliances that strengthen response and product security.
- Understand we cannot secure the planet alone.
- Change rules of the game by influencing the influencers.
- Observe & understand the vulnerability brokerage business model – or encourage the evolution to the next step.
- Provide security researchers access to programs, tools and opportunities that give them a legitimate outlet for their skills.

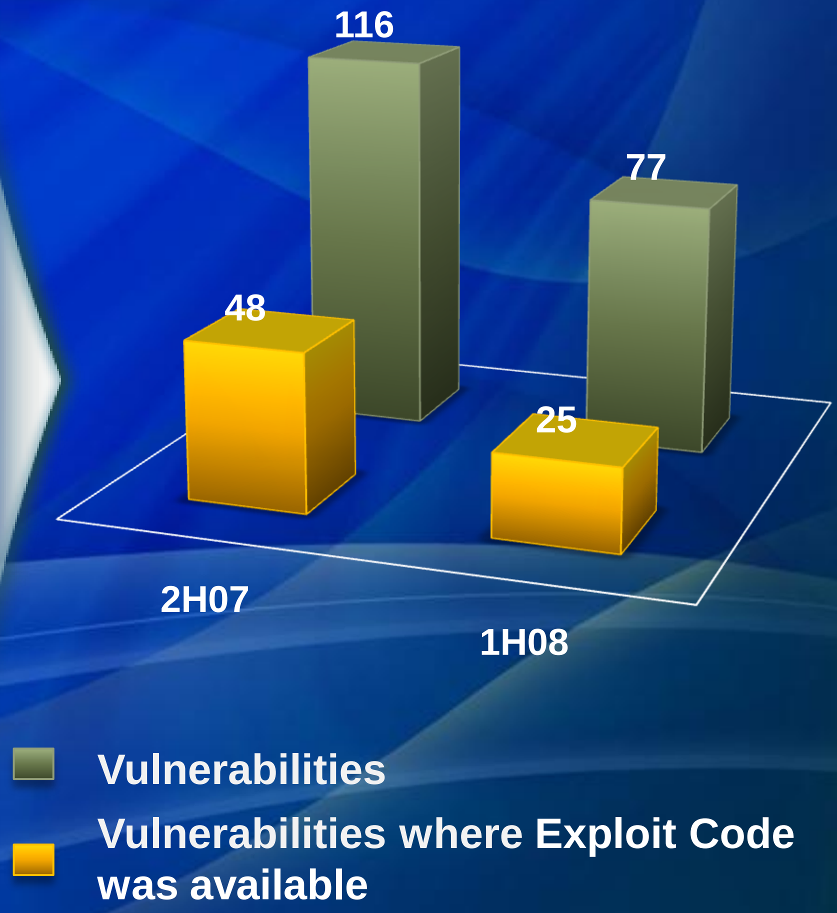
# Microsoft Active Protections Program (MAPP)

- New program for security software providers
- Members of MAPP receive security vulnerability information from MSRC in advance of monthly security update
- Members can provide updated protections to customers via their security software or devices
  - Antivirus
  - Network-based intrusion detection systems
  - Host-based intrusion prevention systems.

# Microsoft Vulnerability Exploits



- ***While number of vulnerabilities Y/Y remains high, the ratio of exploit code available for these vulnerabilities remains steady & is even on a slight decline***



# Understanding the Severity

*Bulletin ratings assume a determined and skilled attacker*

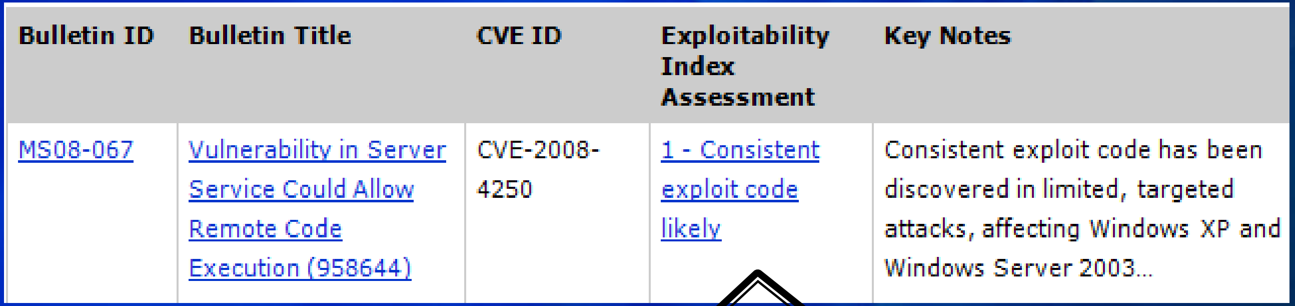
Critical

Important

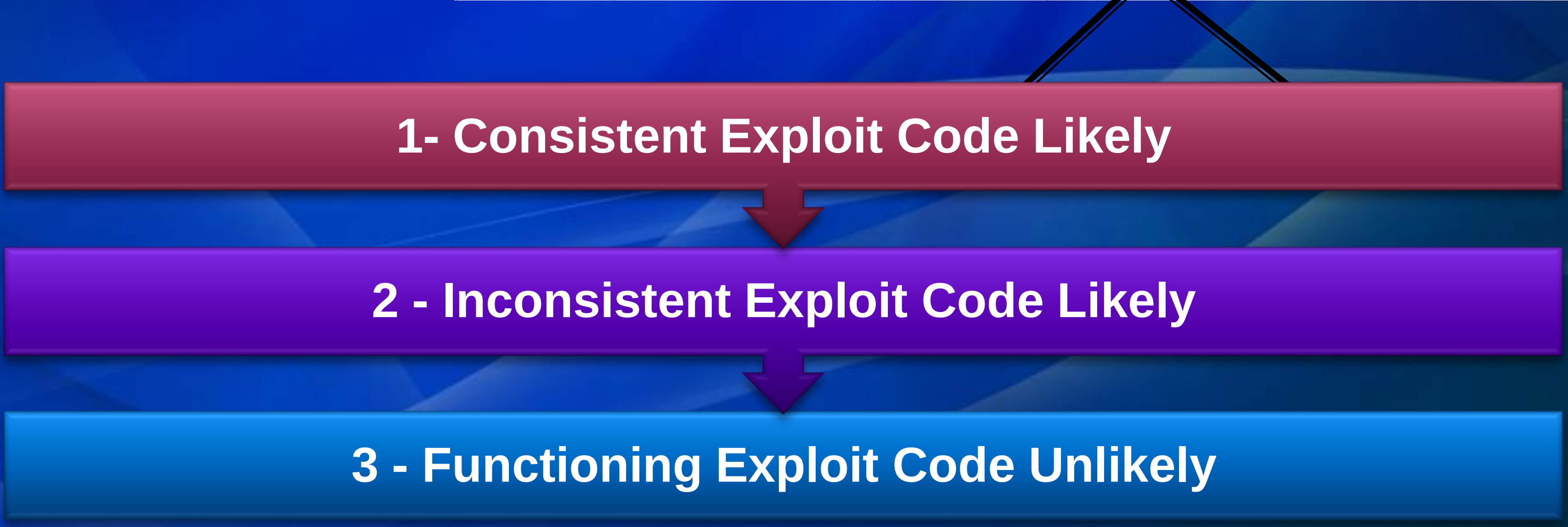
Moderate

Low

*Exploitability Index provides context*



| Bulletin ID | Bulletin Title | CVE ID | Exploitability Index Assessment | Key Notes |
|---|---|---|---|---|
| MS08-067 | Vulnerability in Server Service Could Allow Remote Code Execution (958644) | CVE-2008-4250 | 1 - Consistent exploit code likely | Consistent exploit code has been discovered in limited, targeted attacks, affecting Windows XP and Windows Server 2003... |

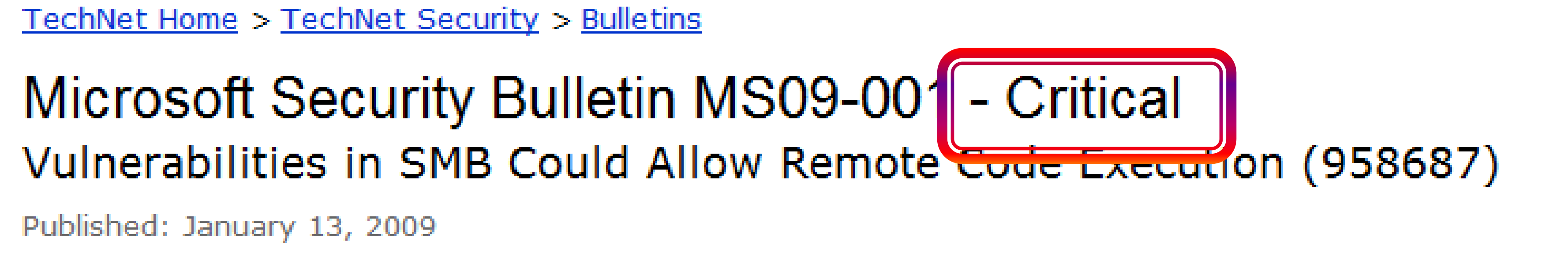


1- Consistent Exploit Code Likely

2 - Inconsistent Exploit Code Likely

3 - Functioning Exploit Code Unlikely

# Exploitability Index and Bulletin Severity ratings



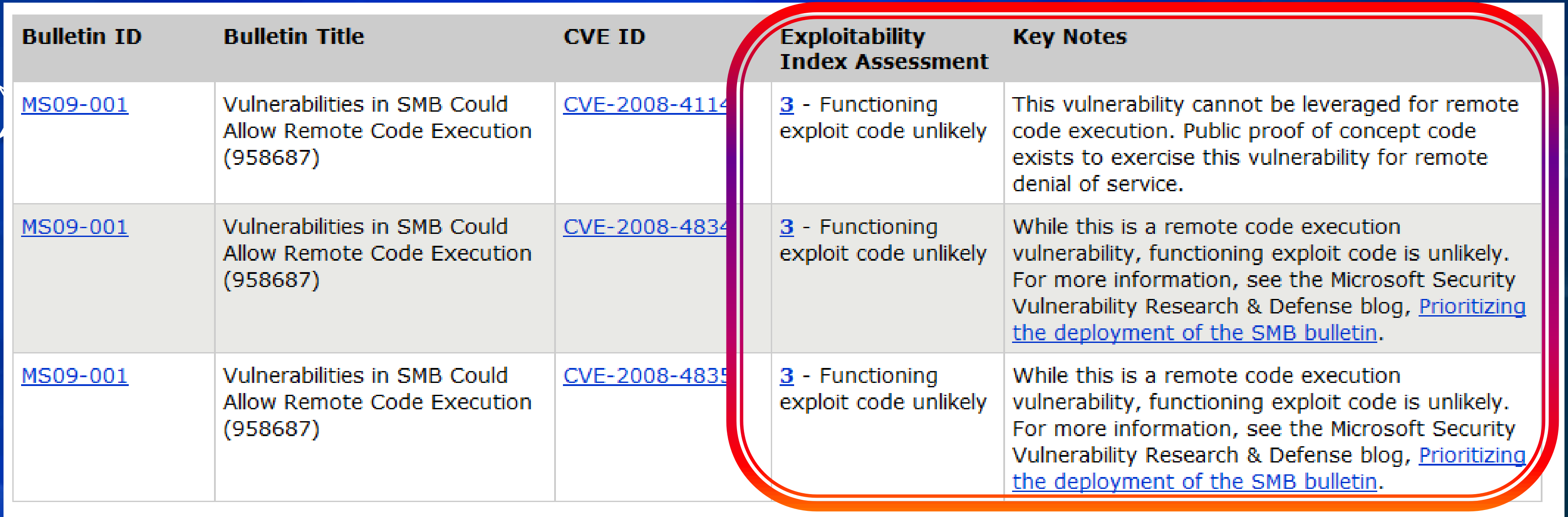
TechNet Home > TechNet Security > Bulletins

Microsoft Security Bulletin MS09-001 - Critical

Vulnerabilities in SMB Could Allow Remote Code Execution (958687)

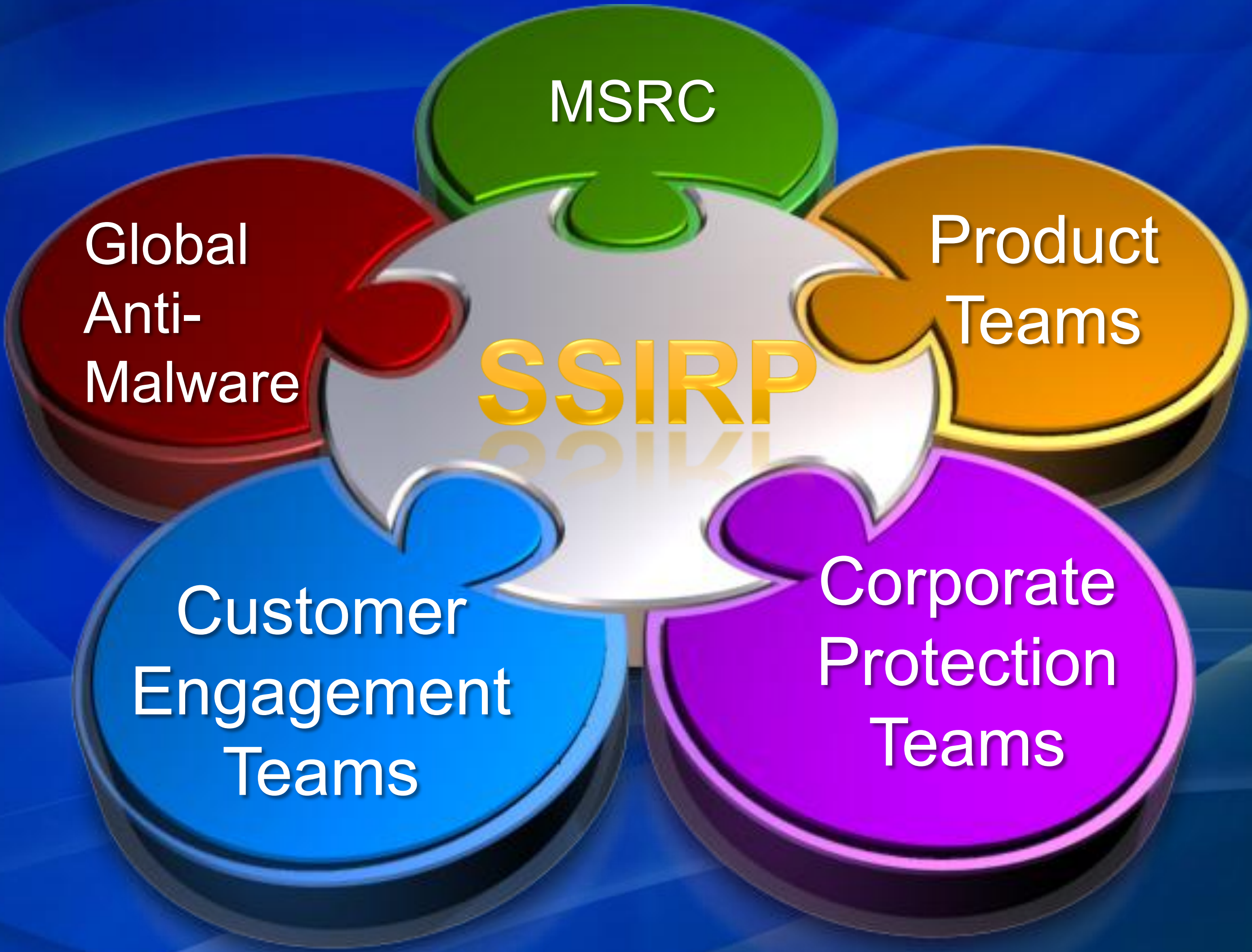
Published: January 13, 2009

- Developed in response to customer requests for additional information to further evaluate risk

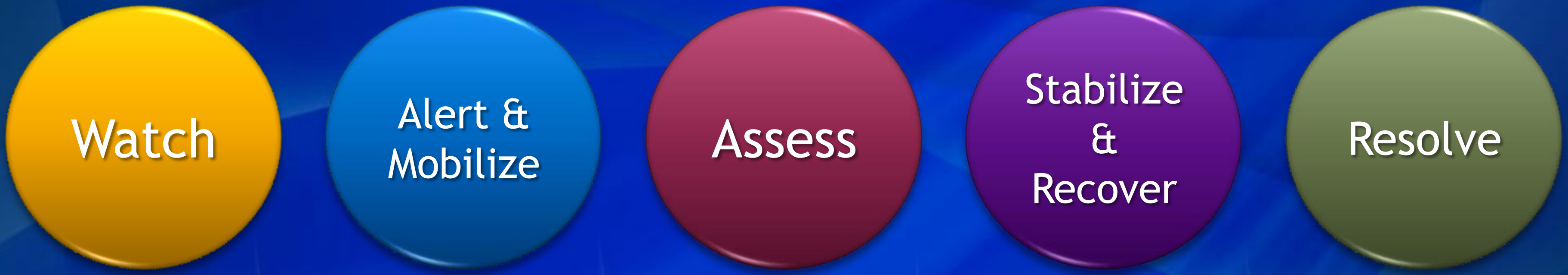


| Bulletin ID | Bulletin Title | CVE ID | Exploitability Index Assessment | Key Notes |
|---|---|---|---|---|
| MS09-001 | Vulnerabilities in SMB Could Allow Remote Code Execution (958687) | CVE-2008-411 | 3 - Functioning exploit code unlikely | This vulnerability cannot be leveraged for remote code execution. Public proof of concept code exists to exercise this vulnerability for remote denial of service. |
| MS09-001 | Vulnerabilities in SMB Could Allow Remote Code Execution (958687) | CVE-2008-483 | 3 - Functioning exploit code unlikely | While this is a remote code execution vulnerability, functioning exploit code is unlikely. For more information, see the Microsoft Security Vulnerability Research & Defense blog, Prioritizing the deployment of the SMB bulletin. |
| MS09-001 | Vulnerabilities in SMB Could Allow Remote Code Execution (958687) | CVE-2008-483 | 3 - Functioning exploit code unlikely | While this is a remote code execution vulnerability, functioning exploit code is unlikely. For more information, see the Microsoft Security Vulnerability Research & Defense blog, Prioritizing the deployment of the SMB bulletin. |

# Coordinating Incidents



# Phases of an Incident Response



## Watch

- Default Stage; Ongoing
- Teams watching for possible incidents

## Alert & Mobilize

- Crisis Leads Alerted
- Incident Triaged
- Mobilize Global security response teams and support groups – two main groups:
  - Emergency Engineering Team
  - Emergency Comms Team

## Assess

- Assess situation and technical information available
- Conduct investigation
- Watch partners look for  signs of activity
- Plan of record established

## Stabilize & Recover

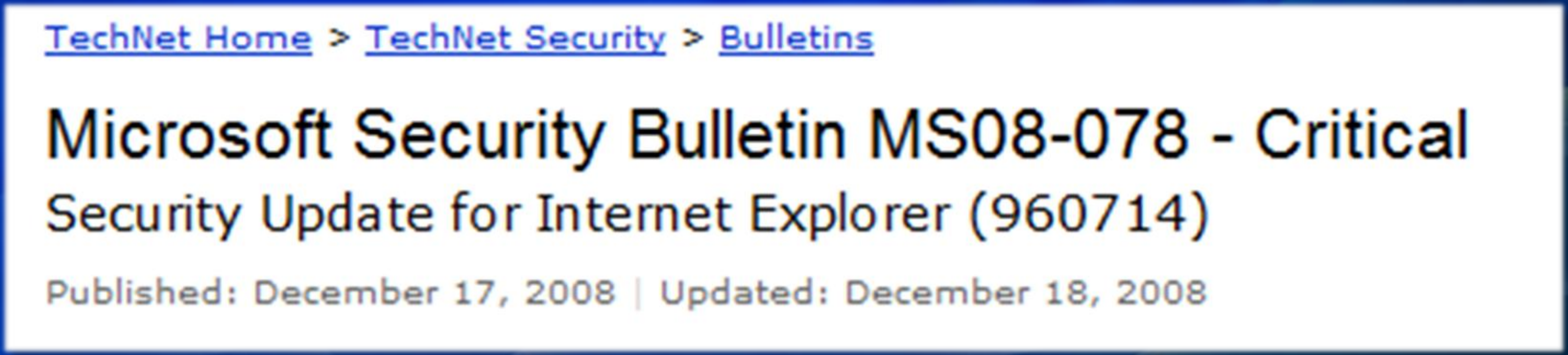
- Product Teams execute Plan of record
- Internal & External Comms prepared
- Insurance Package may be released

## Resolve

- Appropriate solution is provided to customers, such as a security update, tool or fix
- Conduct internal process reviews and gather lessons learned

# Case Walkthrough

- **MS08-078**
  - Internet Explorer Security Vulnerability
  - XML DataBinding
  - Critical severity
  - Out-of-Band Release



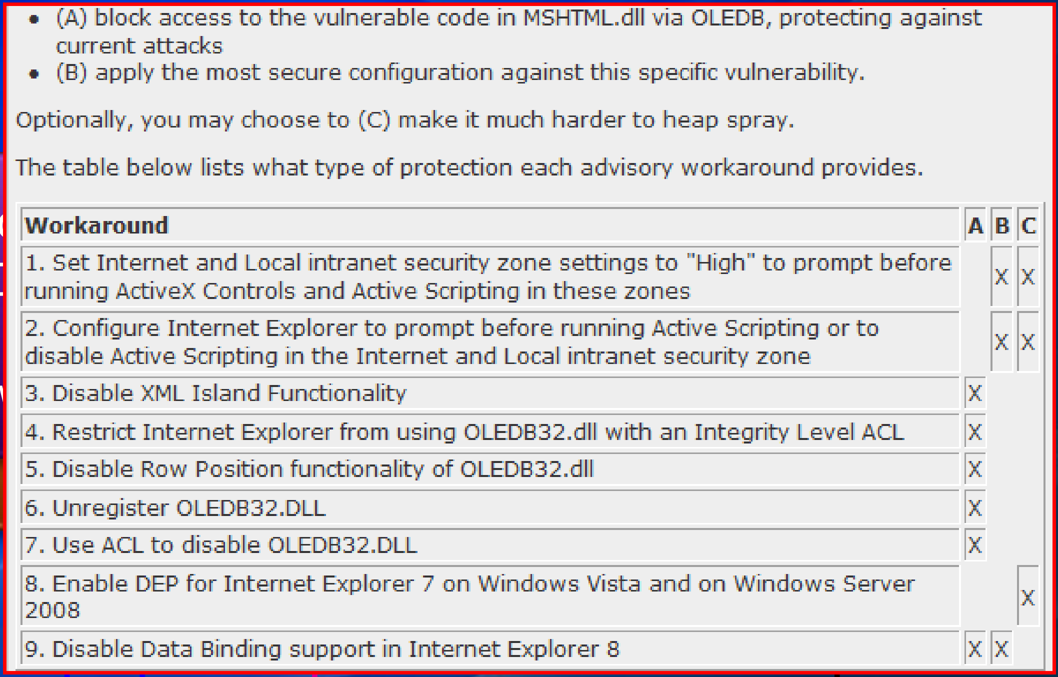
TechNet Home > TechNet Security > Bulletins

Microsoft Security Bulletin MS08-078 - Critical

Security Update for Internet Explorer (960714)

Published: December 17, 2008 | Updated: December 18, 2008

# Internal Process for MS08-078

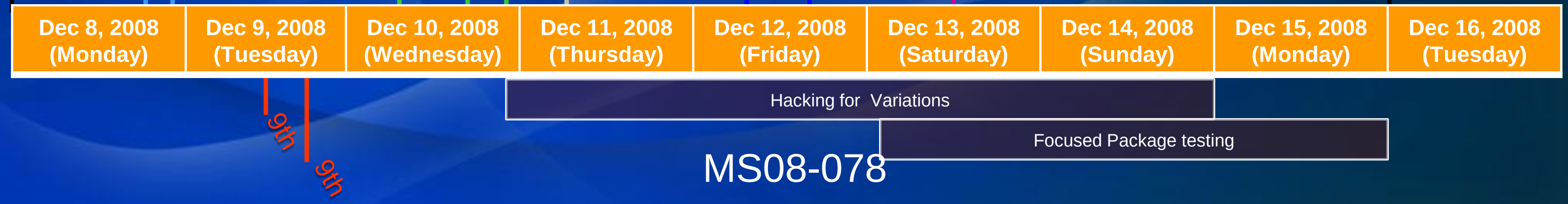


- (A) block access to the vulnerable code in MSHTML.dll via OLEDB, protecting against current attacks
- (B) apply the most secure configuration against this specific vulnerability.

Optionally, you may choose to (C) make it much harder to heap spray.

The table below lists what type of protection each advisory workaround provides.

| Workaround | A | B | C |
|---|---|---|---|
| 1. Set Internet and Local intranet security zone settings to "High" to prompt before running ActiveX Controls and Active Scripting in these zones | | X | X |
| 2. Configure Internet Explorer to prompt before running Active Scripting or to disable Active Scripting in the Internet and Local intranet security zone | | X | X |
| 3. Disable XML Island Functionality | X | | |
| 4. Restrict Internet Explorer from using OLEDB32.dll with an Integrity Level ACL | X | | |
| 5. Disable Row Position functionality of OLEDB32.dll | X | | |
| 6. Unregister OLEDB32.DLL | X | | |
| 7. Use ACL to disable OLEDB32.DLL | X | | |
| 8. Enable DEP for Internet Explorer 7 on Windows Vista and on Windows Server 2008 | | | X |
| 9. Disable Data Binding support in Internet Explorer 8 | X | X | |



# Summary

- Industry leading and dedicated Security Response Engineering team
- Risk assessment & guidance
- Listen to customers & ecosystem
- Rapid Global Response

# Resources

- Blogs:
  - MSRC Operations: http://blogs.technet.com/msrc/
  - MSRC Engineering http://blogs.technet.com/srd/
- Microsoft Security Web sites: www.microsoft.com/security and www.microsoft.com/technet/security
- Sign up to receive notifications on security updates: www.microsoft.com/security/bulletins/alerts.mspx
- Sign up for the Security Bulletin Web cast: www.microsoft.com/technet/security/bulletin/summary.mspx
- RSS Feeds for Security Bulletins: www.microsoft.com/technet/security/bulletin/secrssinfo.mspx
- Security Advisories: www.microsoft.com/technet/security/advisory
- Security Guidance Center for Enterprises: www.microsoft.com/security/guidance
- Protect Your PC: www.microsoft.com/protect
- MAPP http://www.microsoft.com/security/msrc/mapp/overview.mspx

Microsoft®

Your potential. Our passion.™

The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.