Inside the Microsoft Security Response Process

Meng-Chow Kang, CISSP, CISA
Chief Security & Privacy Advisor
Microsoft Asia Pacific

February 24, 2004
APSIRC, APRICOT 2005

Agenda

- Defining Software Security Vulnerabilities
- The Security Response Process:
  - The Microsoft Security Response Center
  - Triaging Vulnerabilities
  - Working with Finders
  - Creating an update
  - The Bulletin Release Process
- Resources

2

Software Security Vulnerability

- Software is written by humans and will always have a certain level of problems in the code.
  - This is not unique to Microsoft products.
- Sometimes these code problems give rise to a Software Security Vulnerability.
  - What it is:
    - A security exposure caused by the design of the underlying software code that makes it infeasible or difficult – even when using the product properly—to prevent an attacker from usurping privileges on a system, regulating its operation, or compromising data on it.
  - What it is not:
    - Weak passwords
    - Misconfigured systems
    - By-design behaviors not related to code design
    - Weak cipher strength in design (ex: 40 bit vs higher)

3

Microsoft Security Response Center (MSRC)

MSRC Prime Directive:

Protect customers from security vulnerabilities in Microsoft Products

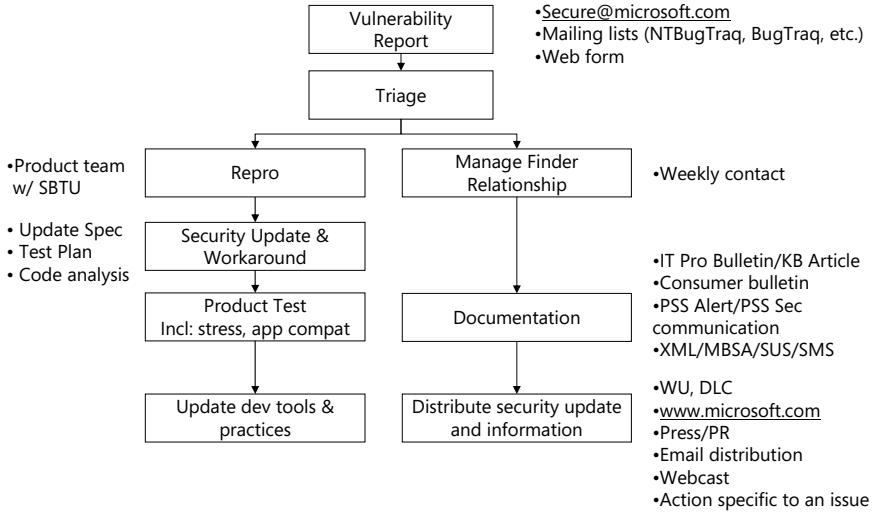
4

MSRC key tasks

- Staff forward facing reporting alias, monitor security lists, work tightly with customers, the field, and PSS.
- Investigate and resolve every vulnerability report
  - Act as customer advocates
  - Single point of coordination and communication
- Communicate and create community with vulnerability finders
- Work with law enforcement, and industry influentials
- Develop and maintain Emergency Response Process
- Work to prevent issues through security engineering and development process changes
- Provide security awareness and expertise

5

Security Response Process



6

Vulnerability Reporting

- Secure@Microsoft.com
  - Direct contact with MSRC
  - 24 hour response SLA to finder
- https://www.microsoft.com/technet/security/bulletin/alertus.aspx
  - Form-based notification
  - More anonymous – sometimes preferred

7

Triaging a vulnerability

- Assessing the report against the Security vulnerability definition
  - Could it be a result of misconfiguration?
  - Is this a bug rather than a security vulnerability?
- Assessing the level of information provided
  - Has the researcher given repro steps?
  - Has the researcher provided affected versions?
- Assessing the impact
  - Is the affected component installed or on by default?
  - Are there any limitations to exploitation of the vulnerability?
    - Denial of service, byte for byte?
    - Is the attack sustained?
    - Is the attack auditable?
    - Code execution privilege limited?
- Assessing the Finder
  - Practices responsible disclosure?
  - Has an existing relationship with MSRC?

8

Working with Finders

- Diverse group
  - Researchers, Academics, Industry specialists, Hobbyists
  - World-wide
- Encourage Responsible Reporting
  - Treat people responsibly and respectfully
  - Negotiation
  - Attribution
- Communications
  - Try to understand their motivation and need
  - Quick response to initial report
  - 2-way – we listen as much as we talk
  - Regular progress updates – making them part of the team
- Building community
  - Let them know Microsoft = individuals

9

Creating the fix

- Product Team investigates repro with test and determine affected code
- Through code review, find and fix similar vulnerabilities in the same code
- Generate Private Fix for test to verify
- After private is verified by test, code review is completed (core or SE counterpart)
- Patch Spec completed at this time
- War Approval & Checkin (all trees applicable)

10

Code Review

- Parallel to testing, Secure Windows Initiative Attack Team and Product Teams conduct code reviews.
  - Investigate the impact of the vulnerability
  - Try to find variants
  - Conduct a further investigation of surrounding code and design
- *This can result in changes to the security update which might reset testing!*

11

Testing Complexity: Internet Explorer

- Take 5 supported versions (IE5.01, IE 5.5, IE6, IE6SP1, IE6SP1 for Win2k3)
- Take 9 supported OS platforms (Windows NT 4.0, Windows 2000 SP2, Windows 2000 SP3, Windows 2000 SP4, Windows XP, Windows XP SP1, Windows XP 64 bit, Windows Server 2003, Windows Server 2003 64bit)
- Take 26 supported languages
- Accounting for shared files, when it's all said and done you get 447 packages to test!
- Testing covers not just application compatibility, but also web rendering

12

WinSE Test Processes: Four levels

- Setup and BVT Testing
  - Install variations across full support matrix
  - Basic functionality testing
- Depth Testing
  - Testing of individual fixes within component area
  - Functionality coverage, security, Interoperability, Code coverage analysis, International etc.
- Integration and Breadth Testing
  - Testing the entire system, all components
  - Application Compatibility, Self host, Stress, Long haul, Performance etc.
- Microsoft IT Feedback

13

Content Creation

Writing the Bulletin

- One author, team effort
  - Bulletins are authored by the MSRC PM in charge of the case
  - Review cycles include MSRC, PSS, Product Team, LCA, Marketing, and an editorial pass
  - MUST be signed off by development and product marketing VP's
- Bulletin design based off customer feedback and includes:
  - Recommended actions
  - Affected software/components
  - Update locations
  - Executive summary
  - Technical description and severity rating
  - Mitigating factors
  - Workarounds (Important!)
  - Frequently asked questions
  - Deployment and update package information
  - Acknowledgements

14

Content Creation
Bulletin Severity Ratings

Critical	Exploitation could allow the propagation of an Internet worm without user action
Important	Exploitation could result in compromise of the confidentiality, integrity, or availability of user 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	Exploitation is extremely difficult, or whose impact is minimal

15

Security Bulletin Advanced Notification Program

- Launched based on customer feedback
- Advance notification on monthly bulletins
- General summary three days prior to release
  - Number of security bulletins
  - Anticipated severity level
  - Overview of affected products
- Assists with preparation & resource planning

More information at www.microsoft.com/technet/security

16

Release Day

Second Calendar Tuesday

- Coordinated release of the following items around 10:00 am on the second Tuesday of every month:
  - Update to Download Center, Windows Update, or Office Update
  - Windows Update text
  - Summary bulletin
  - IT Pro Bulletin
  - Consumer bulletin
  - MSXML file
  - Bulletin mailer notifications
- Same process followed for Out of Band releases

17

Post Release

- Proactive Press and PR
- Email sent to customers who signed up for notification services, Security Notification Service or Security Update Services (www.microsoft.com/security/bulletins/alerts.mspx)
- Security Bulletins Web cast on the Wednesday following the release, 10:00-11:00 AM PT (www.microsoft.com/technet/security/bulletin/summary.mspx)
- Monitoring of security news lists
- Contact with PSS and Windows Update to determine uptake and make corrections as needed
- Bulletin Maintenance

18

Resources

- Security Main Pages
  - http://www.microsoft.com/security - Consumer
  - http://www.microsoft.com/technet/security - IT Pro
  - http://www.microsoft.com/protect - Protect your PC
- A tour of the Microsoft MSRC
  - http://www.microsoft.com/technet/archive/community/columns/security/essays/sectour.mspx
- A day in the life of a Microsoft Security Patch:
  - http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2914659,00.html

19

Microsoft

Your potential. Our passion.™

20