Supporting Security
Inside fixing vulnerabilities at Microsoft

Simon Conant MCSE CISSP
Security Program Manager
PSS Security
Microsoft Corporation
sconant@microsoft.com

Who’s who?

Product Groups
- Program Managers
- Developers
- Test Engineers

Process

<table>
<thead>
<tr>
<th>Evaluation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Issue first received.</td>
</tr>
<tr>
<td>Evaluated &amp; acknowledged to reporter (all reports acknowledged).</td>
</tr>
<tr>
<td>Sent to all possibly affected product group “SI” teams.</td>
</tr>
<tr>
<td>Confirmation of problem (or not). Workarounds, discussions, all the experts pulled in on.</td>
</tr>
<tr>
<td>Full info on problem, associated issues, workarounds, solutions.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Fix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fix architected from step 1</td>
</tr>
<tr>
<td>Fix built for all affected products, platforms, versions, languages.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Test</th>
</tr>
</thead>
<tbody>
<tr>
<td>Fix is tested:</td>
</tr>
<tr>
<td>Fixes all of problem</td>
</tr>
<tr>
<td>Doesn’t break anything else</td>
</tr>
<tr>
<td>All products, versions, platforms, languages</td>
</tr>
<tr>
<td>Broken? Back to step one…</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Release</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field testing</td>
</tr>
<tr>
<td>Packaging</td>
</tr>
<tr>
<td>Documentation</td>
</tr>
<tr>
<td>Publishing</td>
</tr>
</tbody>
</table>
Why does it take so long?

• It’s all about **COMPLEXITY**
  – The products all are very feature-packed, and are therefore very complex
  – We support multiple older versions of products
  – On various platforms
  – And for many languages

• It’s all about **QUALITY**
  – If the fix doesn’t fix ALL of the problem, it’s no good
  – If the fix breaks something else along the way, it’s not helping our customers either
  – We have to do our very best to get it right **first time**

• And we exhaustively test it all.

---

**Workarounds**

- Fix
- Low-impact Workaround
- High impact or partial workaround
- No known / possible workaround

---

**Improvements**

• No more "Under Investigation" black hole
  – Milestones (Public Vulnerability Program)
• Proactive communications
  – PSSSec will own the cases & customer care
• Patch beta testing
• Local security support
• Patch improvements
• Shared Source Programs
Improve the Patching Experience

New Patch Policies

• Extending support to June 2004
  – Windows 2000 SP2
  – Windows NT SP6a

• Non-emergency security patches on a monthly release schedule
  • Allows for planning a predictable monthly test and deployment cycle
  • Packaged as individual patches that can be deployed together
  • Achieves benefits of security rollup with increased flexibility

Patches for emergency issues will still release immediately

---

Improve the Patching Experience

Patch Enhancements

<table>
<thead>
<tr>
<th>Your Need</th>
<th>Our Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reduce patch complexity</td>
<td>Consolidating to 2 patch installers for W2K and higher, Office &amp; Exchange. All patches will behave the same way (SUS 2.0, MSI 3.0)</td>
</tr>
<tr>
<td>Reduce risk of patch deployment</td>
<td>Now: Increased internal testing: customer testing of patches pre-release. Coming: rollback capability for Windows, SQL, Exchange, Office</td>
</tr>
<tr>
<td>Reduce patch size</td>
<td>Now: Reduced patch size by 35% or more. Coming: 80% reduction. (Delta patching technology and improved functionality with MSI 3.0)</td>
</tr>
<tr>
<td>Reduce downtime</td>
<td>Now: 10% fewer reboots on W2K and higher. Coming: 35% fewer reboots on Win 2003 (starting in SP1). Up to 75% reduction for next server</td>
</tr>
<tr>
<td>Extend patch automation to all products</td>
<td>11/03: SMS 2003 offers capability to patch all supported Microsoft platforms and applications. By end of 2004, all MS patches behave the same at installation (MSI 3.0 + SUS 2.0) and available in one place: MS Update</td>
</tr>
</tbody>
</table>

---

Continue Improving Quality

Trustworthy Computing Release Process

<table>
<thead>
<tr>
<th>Design &amp; Specifications</th>
<th>Design</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Review</td>
<td>• Each component team develops threat models, ensuring that design blocks applicable threats</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Development, testing &amp; documentation</th>
<th>Development</th>
</tr>
</thead>
<tbody>
<tr>
<td>M1</td>
<td>Apply security design &amp; coding standards</td>
</tr>
<tr>
<td>M2</td>
<td>Tools to eliminate code flaws (PREfix &amp; PREfast)</td>
</tr>
<tr>
<td>Beta</td>
<td>Monitor &amp; block new attack techniques</td>
</tr>
<tr>
<td>Security Push</td>
<td>Team-wide stand down</td>
</tr>
<tr>
<td>Security Audit</td>
<td>Threat model updates, code review, test &amp; documentation scrub</td>
</tr>
<tr>
<td>Security Response</td>
<td>Analysis against current threats</td>
</tr>
<tr>
<td></td>
<td>Fix newly discovered issues</td>
</tr>
<tr>
<td></td>
<td>Root cause analysis to proactively find and fix related vulnerabilities</td>
</tr>
</tbody>
</table>
Continue Improving Quality
For some widely-deployed, existing products:

Mandatory for all new products:
Critical or important vulnerabilities in the first 90-150 days?

<table>
<thead>
<tr>
<th>TwC release?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
</tr>
<tr>
<td>No</td>
</tr>
</tbody>
</table>

Security Guidance for IT Pros
• Focused on operating a secure environment
• Patterns & practices for defense in depth
• Enterprise security checklist – the single place for authoritative security guidance

• Available Now
  – 17 prescriptive books
  – How Microsoft secures Microsoft guidance & tools
• Later this year and throughout 2004
  – More prescriptive & how-to guides
  – Tools & scripts to automate common tasks

Security Roadmap
Today
Guidance
Monthly patch releases
Guidance & training
How Microsoft runs Microsoft
SUS 2003

0–3 months
Tools & Patching
2 patch locations:
Rollup
Patching enhancements
SUS 3.0
More guidance

3–6 months
Shields
Remote technologies for client and server
“Ad Update”
Further patch improvements

Future
Next-Generation Security
Integrated host security technologies
NGSCB
Windows hardening
Shields

Monthly patch releases
Guidance & training
How Microsoft runs Microsoft
SUS 2003

2 patch locations:
Rollup
Patching enhancements
SUS 3.0
More guidance

Remote technologies for client and server
“Ad Update”
Further patch improvements

Integrated host security technologies
NGSCB
Windows hardening
Shields
Where else we’re involved

- Security patches & tools
- Virus
- Crisis support
- Privacy
- Hacking and IR
- Gov’t & Law Enforcement Liaison
- Anti-spam & computer crime, Legal
- Press/PR/outreach/communications

How to get in touch

- Via your existing MS contact/relationship
- Mailto:sconant@microsoft.com
- +49-175-584 4290