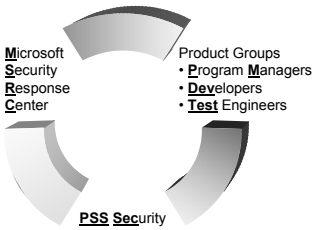
Supporting Security

Inside fixing vulnerabilities at Microsoft®

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

Who's who?



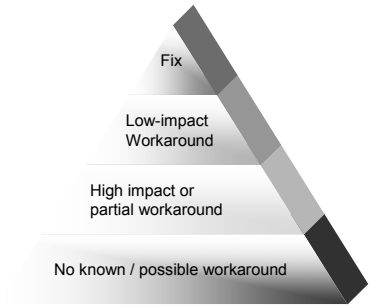
Process

Evaluation	Issue first received. Evaluated & acknowledged to reporter (all reports acknowledged). Sent to all possibly affected product group "SI" teams. Confirmation of problem (or not). Warteams, discussions, all the experts pulled in on it. Full info on problem, associated issues, workarounds, solutions.
Fix	Fix architected from step 1 Fix built for all affected products, platforms, versions, languages.
Test	Fix is tested: -Fixes all of problem -Doesn't break anything else -All products, versions, platforms, languages Broken? Back to step one…
Release	Field testing Packaging Documentation Publishing

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



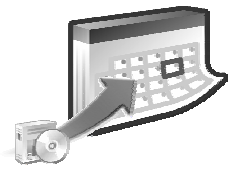
Improvements

- 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

Your Need	Our Response
Reduce patch complexity	**Consolidating to 2 patch installers for W2K and higher, Office & Exchange. All patches will behave the same way** (SUS 2.0, MSI 3.0)
Reduce risk of patch deployment	**Now : Increased internal testing; customer testing of patches pre- release.** **Coming: rollback capability for Windows, SQL, Exchange, Office**
Reduce patch size	**Now: Reduced patch size by 35% or more. Coming: 80% reduction.** (Delta patching technology and improved functionality with MSI 3.0)
Reduce downtime	**Now: 10% fewer reboots on W2K and higher** **Coming: 30% fewer reboots on Win 2003 (starting in SP1). Up to 70% reduction for next server**
Extend patch automation to all products	**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**

Continue Improving Quality

Trustworthy Computing Release Process

Design docs & specifications	Design	Security Review	• Each component team develops threat models, ensuring that design blocks applicable threats
Development, testing & documentation	Development: M1	Develop & Test	• Apply security design & coding standards • Tools to eliminate code flaws (PREfix & PREfast) • Monitor & block new attack techniques
	Development: M2 / Mn / Beta	Security Push	• Team-wide stand down • Threat model updates, code review, test & documentation scrub
Product	Release	Security Audit	• Analysis against current threats • Internal & 3rd party penetration testing
Service Packs, QFEs	Support	Security Response	• Fix newly discovered issues • Root cause analysis to proactively find and fix related vulnerabilities

Continue Improving Quality

For some widely-deployed, existing products:

Mandatory for all new products:

Critical or important vulnerabilities in the first…

	…90 days	…150 days	TwC release?
Windows Server 2003	13	23	No
Windows Server 2003 SP1	6	9	Yes

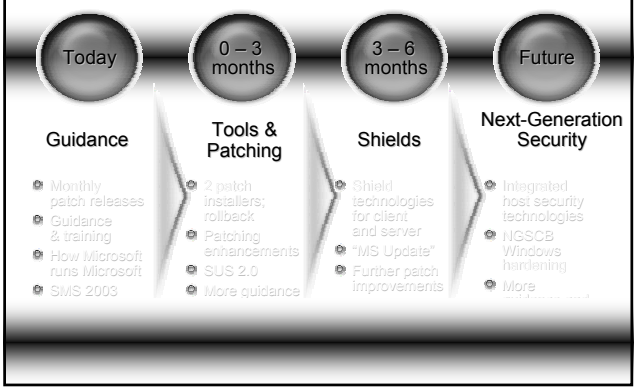
Security Guidance for IT Pros

- Focused on operating a secure environment
- Patterns & practices for defense in depth
- Enterprise security checklist – the single place for authoritative security guidance

patterns & practices

- 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



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