

# September 2006 Security Updates

© 2006 Sûnnet Beskerming Pty. Ltd.

# Our Background

- Quietly achieving
- Reaching more than 400 million people
- Multiple services
- World class advice and content
- Leading research and development services
- Acting global, thinking local

# MS06-040 - Critical

- Server Service (RPC)
- Arbitrary Code Execution
- Being exploited in the wild
- Re-release due to system instability issues
- Perimeter & host firewalls to mitigate
- Block TCP/139, TCP/445 as workaround

# MS06-042 - Critical

- Internet Explorer Cumulative
- Multiple fixes
- Worst case - arbitrary code execution
- Replaces MS06-021 (and some earlier)
- Re-release due to introduced major flaw
- Non-patch mitigation causes issues

# MS06-052 - Important

- Windows 2000, XP, 2003
- PGM - remote code execution
- Protocol implementation bug
- Network packet can be used to exploit
- No non-patch mitigation
- Requires MSMQ to be manually installed

# MS06-053 - Moderate

- Windows 2000, XP, 2003
- Indexing Service - script execution
- Only within context of current user
- Non-patch mitigation can cause issues
- Replaces MS05-003
- Requires some victim interaction

# MS06-054 - Critical

- Microsoft Office 2000, XP (2002), 2003
- Arbitrary code execution in Publisher
- Only installed with Professional versions
- May be exploited via web content
- Victim interaction required
- Can no longer use Publisher 2.0 files

# Contact Us

- **Online**

- *<http://www.beskering.com>*

- **Email**

- *[info@beskering.com](mailto:info@beskering.com)*

- **Telephone**

- *+61 (0)410 707 444*



# Questions



# Thank You

© 2006 - Sûnnet Beskerming Pty. Ltd.