

How Will Cracking Evolve?

The Discovery of MS05-036 Vulnerability

Yu, Chi-Sheng (csyu@icst.org.tw)

Information and Communication Security Technology Center
Chinese Taipei

Who We Are

- ICST (*Information & Communication Security Technology Center*)
 - Founded in 2000
 - CSIRT of public sector
 - IT Security Awareness Promotion and Training
 - Vulnerability Scanning & Penetration Testing
 - Incident Report and Handling
 - Malicious Code Analysis
 - Security Operation Center
 - Intrusion Alert and Advisory Issuance

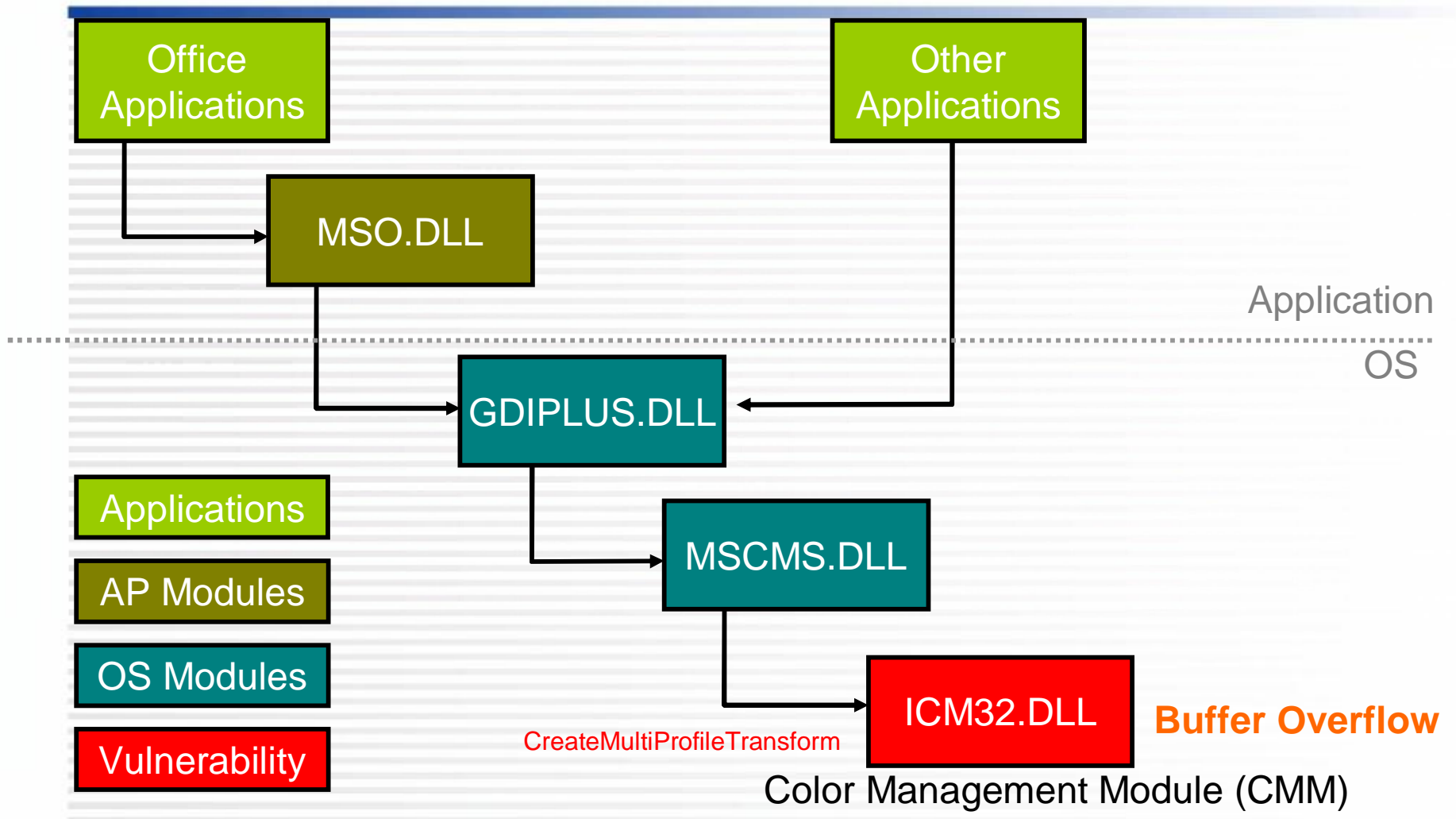
Malicious Code Analysis

- Experiences for Malicious Code Analysis
 - In the past two years, ICST started to collect suspicious emails with Microsoft Office attachments
 - Those malicious MS-Office documents usually exploit well known vulnerabilities to install spywares or backdoors
 - Most of these installed programs are un-detectable to AV software

Discovery of An Unknown Vuln.

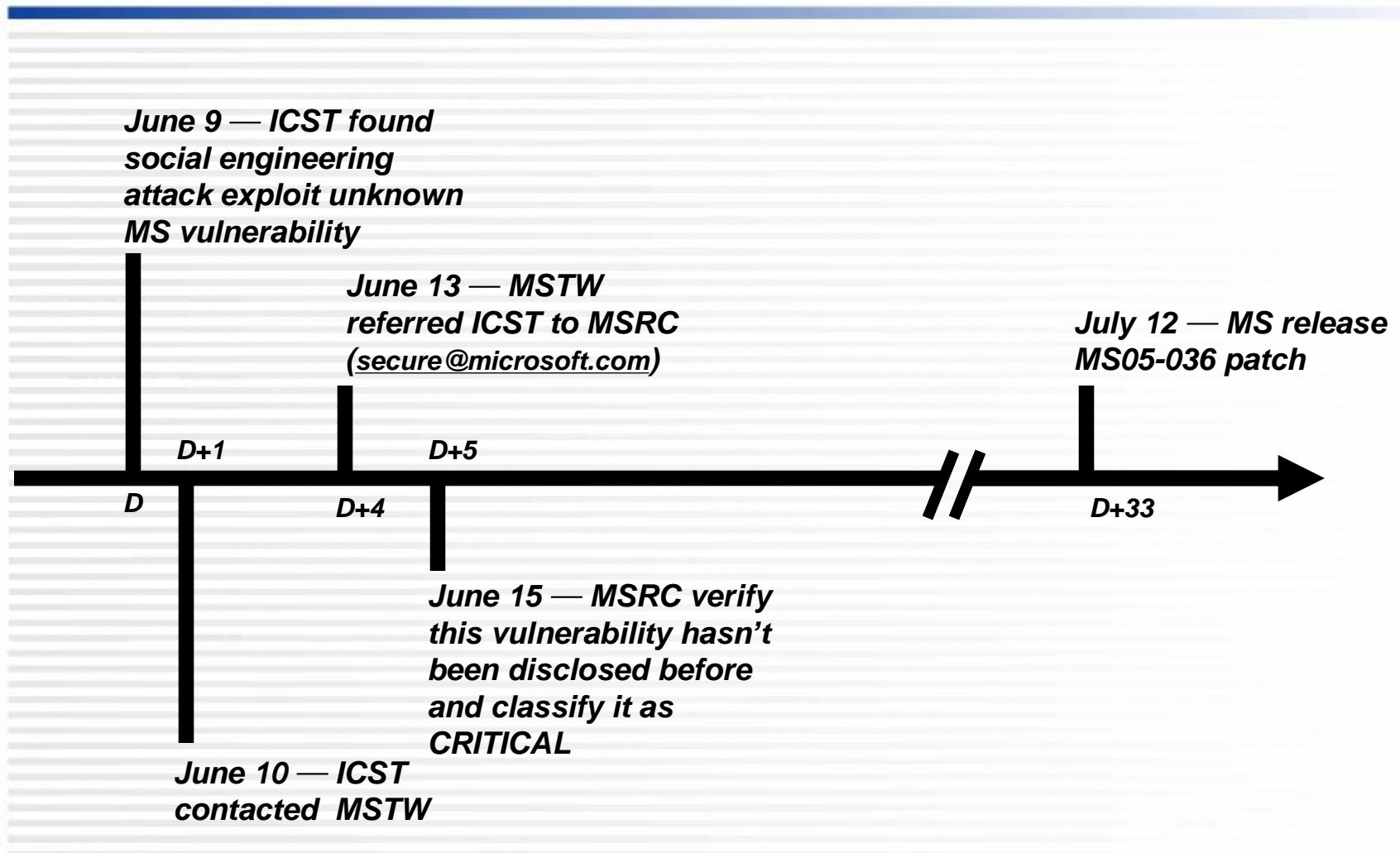
- On June 9, 2005, a suspicious email caught our attention. The malicious program contained in the attachment can be installed even in a fully patched environment
- Analysis Process
 - Static analysis
 - Found an abnormal image in the attached MS WORD file
 - Dynamic analysis with virtual machines
 - On fully/partial patched environments
 - 3rd party programs to monitor registry, file system and network connections (e.g. RegMon, FileMon, windump)
 - Reversed engineering
 - Found an undisclosed vulnerability in “icm32.dll” component which allow this installation

Discovery of An Unknown Vuln.





MS05-036 Handling Process



Microsoft Security Bulletin MS05-036 Vulnerability in Microsoft Color Management Module Could Allow Remote Code Execution (901214)

Issued: July 12, 2005
Updated: July 20, 2005
Version: 1.1

Summary

Who should read this document: Customers who use Microsoft Windows

Impact of Vulnerability: Remote Code Execution

Maximum Severity Rating: Critical

Recommendation: Customers should apply the update immediately.

Security Update Replacement: None

Caveats: None

Tested Software and Security Update Download Locations:

Affected Software:

- Microsoft Windows 2000 Service Pack 4 – [Download the update](#)
- Microsoft Windows XP Service Pack 1 and Microsoft Windows XP Service Pack 2 – [Download the update](#)
- Microsoft Windows XP Professional x64 Edition – [Download the update](#)
- Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1 – [Download the update](#)
- Microsoft Windows Server 2003 for Itanium-based Systems and Microsoft Windows Server 2003 with SP1 for Itanium-based Systems – [Download the update](#)
- Microsoft Windows Server 2003 x64 Edition – [Download the update](#)
- Microsoft Windows 98, Microsoft Windows 98 Second Edition (SE), and Microsoft Windows Millennium Edition (ME) – Review the FAQ section of this bulletin for details about these operating systems.

Acknowledgments

Microsoft [thanks](#) the following for working with us to help protect customers:

- Shih-hao Weng of [Information & Communication Security Technology Center \(ICST\)](#) for reporting the Color Management Module Vulnerability (CAN-2005-1219).

Concluding Remarks

- What we observed in this case
 - MS05-036 was classified as Extremely Critical by Secunia (<http://secunia.com/advisories/16004/>)
 - The exploit of un-disclosed vulnerability adds another dramatic magnitude of difficulties in handling zero-day attack
 - Attack using social engineering and focus on certain group of end users and keep low profile can be more beneficial to crackers

Concluding Remarks

- What we expect
 - Establish efficient and formal vulnerability handling channel between major software manufactures
 - In addition to educate end users, more automatic and behavior-based anti-malicious software tool are needed
 - Programmers and architect should be certified to secure coding and design criteria respectively

Thank You !