Upcoming iDefense Exclusive Vulnerabilities

The following are the iDefense Exclusives which may be part of the next Microsoft Patch Tuesday, scheduled for June 13. iDefense customers have been provided workarounds for these issues as far as 146 days in advance of public notification.

The first two are both file format related vulnerabilities similar to .WMF vulnerability.

440843 - Microsoft Windows Media Player PNG Chunk Decoding Stack-based Buffer Overflow Vulnerability

iDefense Customers Notified on – Feb. 22, 2006

This vulnerability is a stack-based buffer overflow in Windows Media Player (WMP). WMP is a trusted control which loads without prompting in IE and Firefox. This means the vulnerability can be exploited remotely just by visiting a Web page. This vulnerability could allow remote access to a network as the user who was exploited.

Possible workarounds include either removing or deregistering a library that Windows uses for displaying images; MS06-005 suggested this workaround. Side effects of this include, some programs that display images or movies not working properly.

438986 - Microsoft Internet Explorer ART File Parsing Heap Corruption Vulnerability

iDefense Customers Notified on – Feb. 13, 2006

This vulnerability was received thru the VCP (Vulnerability Contributor Program) and does not require any additional software. A malformed ART format image file can be loaded from a Web page and overwrite memory in such a way as to call any code an attacker wants to put there. This vulnerability could allow remote access to a network as the user who was exploited.

Suggested workaround includes removal of the system files used to display this image format.

433419 - Microsoft Windows MRXSMB.SYS MRxSmbCscIoctlOpenForCopyChunk Buffer Overflow Vulnerability

iDefense Customers Notified on – Jan. 17, 2006

This is a local privilege elevation using internal functionality of the Windows file sharing functions. There is a flawed check for the request, which allows the buffer overflow to occur in the kernel. An exploit for this would allow a local attacker (or a remote attacker who managed to get in through another method) a method of gaining complete control of the machine and the unrestricted ability to perform any operation the computer is capable of. As the overflow is in the kernel, any protections the kernel enforces could be ignored.

This vulnerability exists in core functionality of the windows file system and thus any workaround would most likely adversely affect required functionality.

433418 - Microsoft Windows MRXSMB.SYS MrxSmbCscIoctlCloseForCopyChunk Denial of Service Vulnerability

iDefense Customers Notified on – Jan. 17, 2006

This vulnerability is related the previous one, but does not allow code execution. It allows a thread to be created in a process that makes it impossible for some anti-virus engines to remove the file. The impact of this vulnerability is lower than all the others. While the file itself cannot be removed and the process cannot be completely killed, what remains of the process is a single thread which has locked up waiting for resources to be freed, which were never allocated.

Again, this vulnerability exists in core functionality of the windows file system and thus any workaround would most likely adversely affect required functionality.