

New IE 0-day Vulnerability **createTextRange() function Remote Code Execution Exploit**

Introduction

A vulnerability was found in Microsoft Internet Explorer HTML Rendering Engine which can allow remote code execution. An attacker can exploit this vulnerability by creating a specially crafted script and uploading it to a malicious website.

The vulnerability is in the way Internet Explorer calls createTextRange() function from specific types of Input objects: Checkbox, Radio and Image. According to the MSDN documentation, Internet Explorer should not allow these calls.

Instead, a memory corruption occurs and the browser jumps to an OS specific memory position which then can be exploited to execute code from a remote computer by injecting malicious code to the heap.

Threat level: Critical (Remote System Compromise).

Status: Patched. Microsoft Security Bulletin [MS06-013](#)

Affected Versions

- Internet Explorer 6 Service Pack 1 on Microsoft Windows 2000 Service Pack 4
- Internet Explorer 6 Service Pack 1 on Microsoft Windows XP Service Pack 1
- Internet Explorer 6 for Microsoft Windows XP Service Pack 2
- Internet Explorer 6 for Microsoft Windows Server 2003 and Microsoft Windows Server 2003 Service Pack 1
- Internet Explorer 6 for Microsoft Windows Server 2003 for Itanium-based Systems, Microsoft Windows Server 2003 with SP1 for Itanium-based Systems
- Internet Explorer 6 for Microsoft Windows Server 2003 x64 Edition, and Microsoft Windows XP Professional x64 Edition

Attack Vector

- Internet Explorer is a common attack vector for this vulnerability. It requires Active Scripting to be enabled.

Protection

- Vital Security™ Web Appliance customers are protected against this vulnerability.

Finjan's Solution

Utilizing its patented behavior-based security technologies, Finjan delivers the ONLY proactive content security solution capable of protecting companies from new, unknown attacks arriving via the web the first time they strike. Using this patented technology, Finjan's Vital Security™ solutions provide superior protection against complex web-borne attacks, such as Spyware, Phishing/Pharming, Trojans and malicious code.