



Viewfinity Privilege Management Mitigates Microsoft Patch Vulnerabilities

By Dwain Kinghorn

© Viewfinity 2011

A decorative graphic at the bottom of the page, consisting of several overlapping, semi-transparent, light blue and grey geometric shapes that create a sense of depth and movement. The shapes are arranged in a horizontal line, with some appearing to recede into the background and others coming forward.

2011

TABLE OF CONTENTS

Microsoft Patches and Privilege Management..... 3
Analysis of Microsoft Security Bulletins..... 4
Why Privilege Management is a Key in Malware Protection 8
About the Author 11

Microsoft Patches and Privilege Management

IT professionals that support Windows desktops are well aware of “Patch Tuesday”. This is the day every month when Microsoft releases their patch updates for the Microsoft products. Month after month there are new vulnerabilities that are reported to Microsoft and Microsoft releases the updates that address the vulnerabilities on a regular monthly cadence.

As part of the process of releasing the patches, Microsoft provides an executive summary to provide details about each security bulletin. In this overview, Microsoft highlights those vulnerabilities that are mitigated when local logged on users do not have administrative rights. Here is an example for security bulletin MS-10-090, published in December of 2010 (text highlighted for clarity) . See:

<http://www.microsoft.com/technet/security/bulletin/MS10-090.mspx>

Microsoft Security Bulletin MS10-090 - Critical Cumulative Security Update for Internet Explorer (2416400)

Published: December 14, 2010 | Updated: January 04, 2011

Version: 1.1

General Information

Executive Summary

This security update resolves four privately reported vulnerabilities and three publicly disclosed vulnerabilities in Internet Explorer. The most severe vulnerabilities could allow remote code execution if a user views a specially crafted Web page using Internet Explorer. **Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights.**

A review of all the software updates that Microsoft released in 2010 demonstrates that month after month there are vulnerabilities in Windows, Internet Explorer, and Microsoft Office that are mitigated when the user is not running with administrator privileges. Because Windows, Internet Explorer, and Office are so common, the benefits of not running with administrator rights are of value in almost any organization. Simply stated, when end users do not have administrator rights, the desktop is less vulnerable to a variety of malware. Desktop lockdown compliments other security measures and provides an additional layer of defense against malware.

Recent analysis from Gartner highlights the need for organizations to utilize multiple layers of defense on the endpoints to protect against malware.

- ✓ Malware continues to become more sophisticated, damaging and effective, and is increasingly targeted at specific organizations.
- ✓ Traditional signature-based approaches are increasingly less-effective, and will become a less-important part of a comprehensive defense in depth strategy.

Emerging Vendors in Malware Control, 2010- 9 December 2010 | ID:G00209586

Privilege management software allows organizations to remove administrator rights from the end user while enabling the end user to still run certain approved operations that require elevated rights. Therefore a privilege management solution is an essential component in organizations to help them balance the requirements for end user productivity and maintain a more secure and stable computing environment.

Analysis of Microsoft Security Bulletins

Each month Microsoft publishes a summary of the software updates that have been released. These releases are made available on the second Tuesday of each calendar month. An example of the summary from December 2010 can be found at:

<http://www.microsoft.com/technet/security/bulletin/ms10-dec.aspx>

Each of the bulletin IDs that are part of the release for that month is referenced in the monthly overview. The details of a bulletin include the degree to which the risk is mitigated when the logged on user does not have administrative rights.

The data in the following table lists only a subset of the bulletins that were released in 2010. The objective isn't to recap each bulletin released in 2010. **The table shows for a given month if there is at least one update that addresses an issue in Microsoft Office, Internet Explorer, or Windows which was mitigated when the user does not have local administrator rights.**

A review of the 2010 data shows that in every month in 2010 there was at least one update published that was mitigated when users don't have administrator rights. In 11 months in 2010 there were multiple updates published that fell into this category.

- ✓ During 2010 there were 9 months in which there was at least one update for Microsoft Windows that addressed issues that were less significant when users didn't have administrative rights.
- ✓ During 2010 there were 7 months in which there was at least one update for Internet Explorer that addressed issues that were less significant when users didn't have administrative rights.
- ✓ During 2010, there were 11 months in which there were updates for Microsoft Office that addressed issues that were less impacted when users didn't have administrative rights.

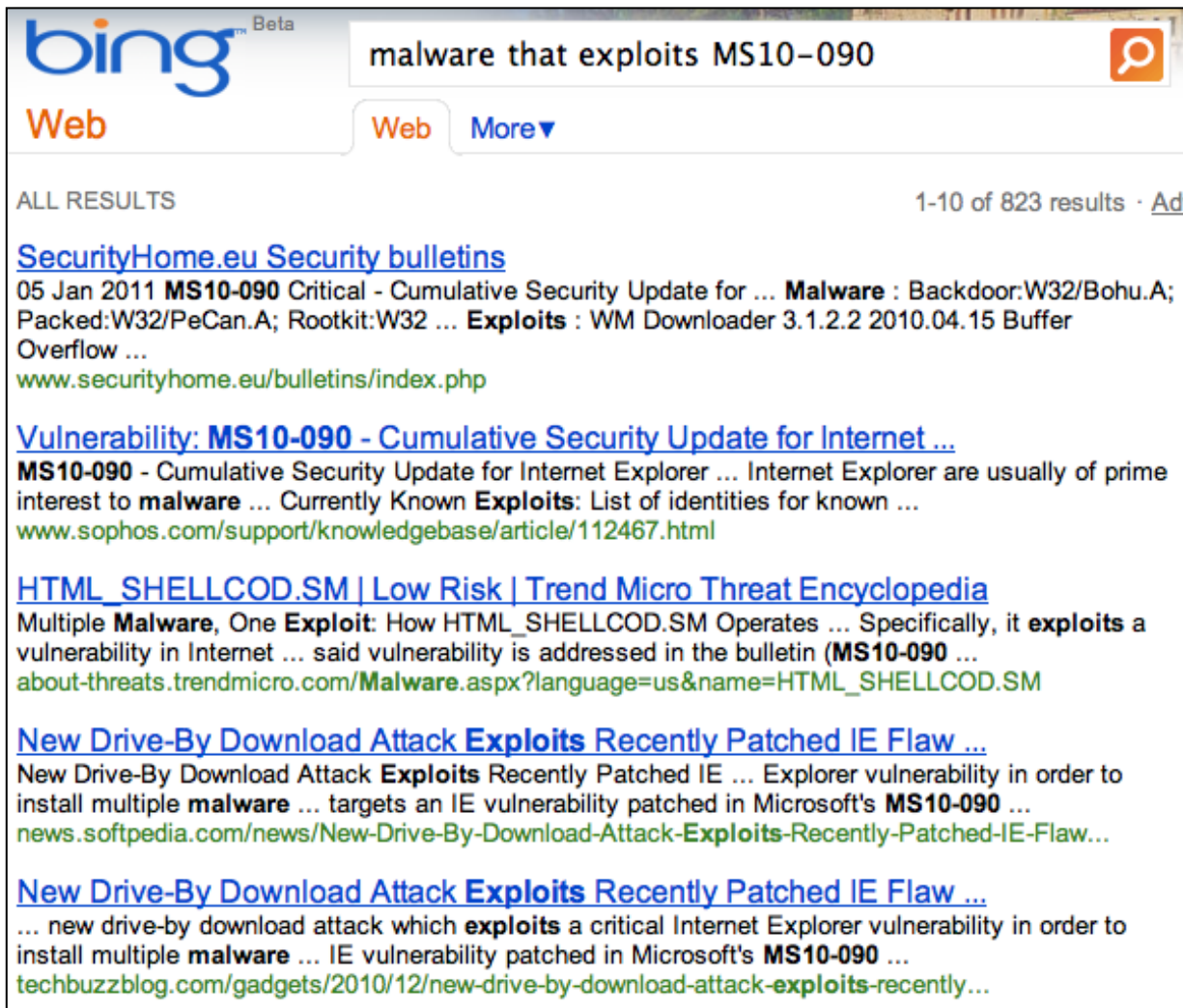
Clearly running without administrator rights is applicable and beneficial to the issues raised month after month.

Month	Bulletin ID	Product	Title
January 2010			
	MS10-001	Windows	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (972270)
	MS10-002	Internet Explorer	Cumulative Security Update for Internet Explorer (978207)
February 2010			
	MS10-013	Windows	Vulnerability in Microsoft DirectShow Could Allow Remote Code Execution (977935)
	MS10-003	Office	Vulnerability in Microsoft Office (MSO) Could Allow Remote Code Execution (978214)
	MS10-008	Internet Explorer	Cumulative Security Update of ActiveX Kill Bits (978262)
March 2010			
	MS10-018	Internet Explorer	Cumulative Security Update for Internet Explorer (980182)
	MS10-016	Windows	Vulnerability in Windows Movie Maker Could Allow Remote Code Execution (975561)
	MS10-017	Office	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (980150)

Month	Bulletin ID	Product	Title
April 2010			
	MS10-026	Windows	Vulnerability in Microsoft MPEG Layer-3 Codecs Could Allow Remote Code Execution (977816)
	MS10-023	Office	Vulnerability in Microsoft Office Publisher Could Allow Remote Code Execution (981160)
May 2010			
	MS10-030	Windows	Vulnerability in Outlook Express and Windows Mail Could Allow Remote Code Execution (978542)
	MS10-031	Office	Vulnerability in Microsoft Visual Basic for Applications Could Allow Remote Code Execution (978213)
June 2010			
	MS10-033	Windows	Vulnerabilities in Media Decompression Could Allow Remote Code Execution (979902)
	MS10-035	Internet Explorer	Cumulative Security Update for Internet Explorer (982381)
	MS10-038	Office	Vulnerabilities in Microsoft Office Excel Could Allow Remote Code Execution (2027452)
July 2010			
	MS10-045	Office	Vulnerability in Microsoft Office Outlook Could Allow Remote Code Execution (978212)
August 2010			
	MS10-046	Windows	Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198)
	MS10-053	Internet Explorer	Cumulative Security Update for Internet Explorer (2183461)
	MS10—056	Office	Vulnerabilities in Microsoft Office Word Could Allow Remote Code Execution (2269638)
September 2010			
	MS10-062	Windows	Vulnerability in MPEG-4 Codec Could Allow Remote Code Execution (975558)

Month	Bulletin ID	Product	Title
	MS10-063	Office	Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2320113)
October 2010			
	MS10-071	Internet Explorer	Cumulative Security Update for Internet Explorer (2360131)
	MS10-076	Windows	Vulnerability in the Embedded OpenType Font Engine Could Allow Remote Code Execution (982132)
	MS10-079	Office	Vulnerabilities in Microsoft Word Could Allow Remote Code Execution (2293194)
November 2010			
	MS10-087	Office	Vulnerabilities in Microsoft Office Could Allow Remote Code Execution (2423930)
December 2010			
	MS10-090	Internet Explorer	Cumulative Security Update for Internet Explorer (2416400)
	MS10-105	Office	Vulnerabilities in Microsoft Office Graphics Filters Could Allow for Remote Code Execution (968095)

A search on the bulletin IDs MS10-090 shows an example of malware that exploits an issue associated with one or the bulletins.



The image shows a screenshot of a Bing search results page. The search query is "malware that exploits MS10-090". The page displays several search results related to security bulletins and malware exploits. The first result is from SecurityHome.eu, dated 05 Jan 2011, titled "SecurityHome.eu Security bulletins". It mentions "MS10-090 Critical - Cumulative Security Update for ..." and lists malware like "Backdoor:W32/Bohu.A; Packed:W32/PeCan.A; Rootkit:W32 ..." and exploits like "WM Downloader 3.1.2.2 2010.04.15 Buffer Overflow ...". The second result is from Sophos.com, titled "Vulnerability: MS10-090 - Cumulative Security Update for Internet ...". It states "MS10-090 - Cumulative Security Update for Internet Explorer ..." and lists "Exploits: List of identities for known ...". The third result is from Trend Micro Threat Encyclopedia, titled "HTML_SHELLCOD.SM | Low Risk | Trend Micro Threat Encyclopedia". It describes "Multiple Malware, One Exploit: How HTML_SHELLCOD.SM Operates ..." and mentions "Specifically, it exploits a vulnerability in Internet ... said vulnerability is addressed in the bulletin (MS10-090 ...". The fourth result is from Softpedia, titled "New Drive-By Download Attack Exploits Recently Patched IE Flaw ...". It states "New Drive-By Download Attack Exploits Recently Patched IE ... Explorer vulnerability in order to install multiple malware ... targets an IE vulnerability patched in Microsoft's MS10-090 ...". The fifth result is from Techbuzzblog.com, titled "New Drive-By Download Attack Exploits Recently Patched IE Flaw ...". It describes "... new drive-by download attack which exploits a critical Internet Explorer vulnerability in order to install multiple malware ... IE vulnerability patched in Microsoft's MS10-090 ...".

Viewfinity Privilege Management is a Key in Malware Protection

Viewfinity Privilege Management enables organizations to define policies that control the rights associated with a set of approved tasks and policies. Privilege management works at a level that is invisible to the end user. Most organizations do not want their users to have to deal with the User Account Control (UAC) dialog box that pops up on the desktop when a non-administrator user runs a task that needs higher rights. Viewfinity Privilege Management solves this problem by enforcing per process policies that are configured on the Viewfinity server.

Security policies that compliment operational standards are recognized as a best practice. A report published by Gartner in 2011 states:

“The convergence of security and operations has been a key theme in client computing for several years. Many security best practices involve standardization, good change management and the enforcement of policies on the endpoint. Desktop organizations have been assuming more security responsibilities, particularly those that are operational.” Publication Date: 20 January 2011/ID Number: G00209766

To enable the effective lockdown of all the desktops, organizations need a solution that works for systems that are outside of the firewall and for machines that may not be regularly connected to Active Directory. Viewfinity Privilege Management does not require the desktop to communicate with Active Directory. The Viewfinity agent is optimized to work in remote and occasionally connected environments that are so common for today’s mobile workforce.

When the locally logged on user does not have administrative rights, the programs and processes that the user runs do not have the rights to be susceptible to many of the vulnerabilities that are referenced in the monthly Microsoft security bulletins.

For example, when a user visits a bad web site, the malware that runs on the system in the context of Internet Explorer is running with the user rights. If the user is not an administrator, then the malware is not as likely to be able to change core system settings or otherwise exploit the vulnerability. This level of protection compliments other endpoint security software such as firewall and anti-virus software.

A number of the attacks that have been designed to exploit the Microsoft vulnerabilities leverage a logged on user’s trust. Organizations both large and small have had issues where a user opens an email from a known email address and clicks on a link that goes to a website with malicious content. Because of the large number of laptop systems that are in most environments, the endpoint may be connecting to bad web sites from outside of the protection of firewalls and content filters that run inside of the corporate network. As a result, so called “socially engineered” malware is much more dangerous when the user is logged on as an administrator on the system because the internet facing application is running with elevated rights.

Viewfinity Privilege Management allows organizations to protect their endpoints from the malware that runs in the user context. There is no need to elevate the privilege level of the browser, mail reader, or other internet facing applications.

While most organizations would like to remove administrator rights, there are a number of end user productivity challenges that occur when this happens. As an example many applications are not compatible, users cannot perform some basic system maintenance tasks, and users are not able to install approved software.

Viewfinity Privilege Management allows the administrator to define specific processes and tasks that will run with elevated rights without any UAC dialog. This combination maintains desktop security without keeping the user from being able to run a number of approved functions that would otherwise require the user to have administrator rights.

A locked down endpoint is less susceptible to malware that exploits the vulnerabilities that are highlighted every month on Patch Tuesday. Privilege management software from Viewfinity bridges the gap between desktop lockdown and end user productivity.

About the Author



Dwain Kinghorn – *Partner at SageCreek*

Dwain's focus is to help companies align their product portfolio with their go to market and business requirements. Prior to SageCreek, Dwain was Vice President at Symantec Corporation and was in charge of the collaboration architecture to ensure multiple Symantec products work together. He was instrumental in the successful adoption of the Altiris platform at Symantec.

Dwain served as the CTO at Altiris from 2000 through the Symantec acquisition in 2007 and oversaw a development team that grew to over 500 people and an engineering budget in excess of \$50M. Dwain knows how to work with diverse teams across the world. He has a strong background in how to manage teams that consist of both employees and outsourced resources across the world. His leadership of the product teams was instrumental in Altiris' products receiving a large number of industry awards.

Dwain was instrumental in evaluating acquisition targets and has had a key role in the M&A process for many transactions. Dwain is a successful entrepreneur having started Computing Edge in 1994. Each year for 6 years Computing Edge experienced greater than 40% growth and each year the operation was profitable. Computing Edge was the recognized leader in solutions that extended Microsoft's management platform.

Prior to Computing Edge, Dwain worked at Microsoft in the Operating System division. Dwain graduated summa cum laude with a degree in Electrical and Computer Engineering.