Microsoft releases tool to block DLL load hijacking attacks

But Microsoft declined to confirm whether any of its own applications are vulnerable

By Gregg Keizer | Computerworld AUGUST 24, 2010

http://www.infoworld.com/d/security-central/microsoft-releases-tool-block-dll-load-hijacking-attacks-016?source=rss_infoworld_news

Microsoft has responded to reports of potential zero-day attacks against a large number of Windows programs by publishing a tool it said would block known exploits.

However, the company declined to confirm whether any of its own applications are vulnerable, saying that it is currently investigating Microsoft-made software.

Monday's **security advisory** was its first public reaction to a wave of reports from researchers that developers have **left a large number of Windows programs open to attack**.

Many Windows applications don't call code libraries -- dubbed "dynamic-link library," or "DLL" -- using the full pathname, but instead use only the filename, giving hackers wiggle room. Criminals can exploit that by tricking the application into loading a malicious file with the same name as the required DLL. The result: Hackers can hijack the PC and plant malware on the machine.

HD Moore, chief security officer at Rapid7 and the creator of the Metasploit penetration testing toolkit, was the first to reveal the potential attacks when he announced last week that he'd found **40 vulnerable Windows applications**. Moore was followed by other researchers who claimed different numbers of at-risk programs, ranging from **over 200** to **fewer than 30**.

Microsoft went to lengths today to tell users that the flaw isn't in Windows.

"We're not talking about a vulnerability in a Microsoft product," said Christopher Budd, a senior communications manager with the company's MSRC, or Microsoft Security Response Center. "This is an attack vector that tricks an application into loading an untrusted library."

Because application developers, not Windows, are to blame, Microsoft can't patch the operating system without crippling an unknown number of programs that run on the platform. Instead, Microsoft and third-party developers must sniff out which of their programs are vulnerable, then patch each separately.

To ward off attacks until then, Microsoft has, as expected, released a tool that blocks the loading of DLLs from remote directories, such as those on USB drives, websites and an organization's network, all possible vectors.

"The tool restricts the loading of remote libraries on a per app [basis] or in a blanket implementation," said Budd. The **tool can be downloaded** using Windows version-specific links in a just-published support document.

Microsoft's tool targets enterprises, not consumers, said Budd, and won't be pushed to customers automatically through the company's Automatic Updates service.

In the advisory, **Microsoft** listed other workarounds customers could take, including blocking outbound SMB (Server Message Block) traffic at the firewall and disabling Windows' built-in Web client. Last week, Moore had recommended users do both, based on his preliminary work.

Budd also argued that the possible exploits spelled out by Moore and others represent a new attack vector, a claim that some researchers rejected.

"This [has been] known since 2000, and I also reported it in 2006," said Israeli researcher Aviv Raff on Twitter Monday. Aviv had revealed a **DLL load hijacking bug** in Internet Explorer 7 (IE7) in December 2006. Microsoft waited until **April 2009** to patch Raff's IE vulnerability.

Microsoft today refused to say whether any of its applications include the programming flaw that would make them vulnerable. "We're going through [our products] and researching," said Budd. "If there are vulnerabilities, we'll address them."

Earlier today, several outside security researchers said they would be interested to know whether any Microsoft software is at risk, which would mean that Microsoft's developers had not followed the company's advice to third-party programmers.

Budd said he couldn't immediately confirm that Microsoft has known of the DLL load hijacking vulnerabilities since at least August 2009, when University of California Davis researcher Taeho Kwon said he contacted the company. Today, Budd said that he understood that Microsoft had been working the problem only for the "past couple of weeks."

If Kwon's timeline is accurate, Microsoft's inability to name which of its products, if any, are vulnerable will likely seem especially odd to researchers.

The MSRC engineering team also published some technical information about the attack vector and the blocking tool on Microsoft's **"Security Research & Defense"** blog Monday.

*Gregg Keizer covers Microsoft, security issues, Apple, Web browsers and general technology breaking news for Computerworld. Follow Gregg on Twitter at **@gkeizer** or subscribe to **Gregg's RSS feed**.*

*His email address is **gkeizer@ix.netcom.com**.*

***Read more about security** in Computerworld's Security Topic Center.*

***Computerworld** is an InfoWorld affiliate.*

ktvorimirglf 11 minutes ago from API http://bit.ly/ao9luG Icons pictures for application designers: Security Toolbar Icons

Exaspring 1 hour ago from ExaSpring Information Services Mod Security Open source Web Application Firewall http://pr9.in/7b

cebu_iphone 1 hour ago from HootSuite freelance iphone dev iPhone Application to stream CCTV/Security Camera feeds by rybrad http://ow.ly/18JkvZ

cebu_iphone 1 hour ago from HootSuite mobile phone iPhone Application to stream CCTV/Security Camera feeds by rybradhttp://ow.ly/18Jkw2

Related Content

Eight Fascinating Facts about DR | White paper

The Role of the Internet in the Propagation of Malware | White paper

NETGEAR® In-The-Cloud Distributed Spam Analysis Technology | White paper

Additional Resources

WHITE PAPER

7 Technologies Behind Ultimate Storage Efficiency

Get the most out of the storage you already own. Download this whitepaper today and examine 7 key technologies behind maximizing your storage efficiency. **Download now »**

WHITE PAPER

Insider Threat Deep Dive Report

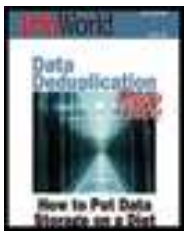
Stop unscrupulous insiders. A clever criminal can lull the boss into believing nothing is amiss. Systems designed to monitor the network for patterns of criminal or destructive behavior are much harder to fool. Learn how to put the right countermeasures in place and vastly reduce the threat posed by insiders. **Download now »**

WHITE PAPER

A Powerful Platform for Virtualization

Examine the 5 unique requirements that virtualization imposes on hardware, and discover how the next generation of HP's ProLiant

server line can deliver virtualized, efficient data centers, rapid ROI and lower operational expenses. **Download now »**



WHITE PAPER

How to Put Data Storage on a Diet

Data storage needs continue to grow unabated, straining backup and disaster recovery systems while requiring more online spindles, using more power, and generating more heat. That leaves IT professionals to search for technology solutions that can at least lighten the load. One solution particularly well-suited to backup and disaster recovery is data deduplication, which takes advantage of the enormous amount of redundancy in business data. With a little help from data deduplication, admins can reduce costs, lighten backup requirements, and accelerate data restoration in the event of an emergency. **Download now »**

EMAIL DE ALERTA DISTRIBUIDO NOS EUA E CANADÁ

From: contacts@bit9.com
To:
Date: Wed, 25 Aug 2010 15:54:42 -0400
Subject: Protect Against Microsoft DLL Load Hijacking

Bit9

Dear Everyone,

Today's reports of the zero-day Microsoft DLL load hijacking attacks highlight how difficult it is to secure Windows systems. Further exacerbating the issue:

- Microsoft cannot fix these issues without breaking functioning systems
- Anti-virus cannot provide signature updates for these zero-day attacks
- Compromised systems cannot be easily identified without visibility into what's running on your endpoints

Download this case study to learn how a US Government agency, targeted by a similar attack, prevents all unapproved files. Bit9 Application Whitelisting is uniquely positioned to stop these kinds of attacks by:

- Blocking hijacked DLLs from execution.
- Preventing unknown malware from running.
- Validating the DLL files are trustworthy and authentic.

Download the Case Study

Best,
Kate Munro
Bit9, Inc

Download Now

De: contacts@bit9.com
Para:
Data: Quarta-feira, 25-ago-2010
Assunto: Proteja-se contra o sequestro da carga das DLLs da Microsoft.

Bit9

Prezados todos:

Hoje os relatórios do "*dia-zero para os ataques visando o sequestro das DLLs em carga da Microsoft*" destacam como é dificil manter os sistemas da Microsoft em segurança. E para piorar ainda mais as coisas:

- A Microsoft não consegue eliminar esses problemas sem que a funcionalidade do sistema seja quebrada.
- Os anti-virus não podem manter atualizadas as assinaturas desses "ataques do dia-zero".
- Os sistemas comprometidos não podem ser facilmente identificados sem que se saiba exatamente o que entrou em execução na memória do computador.

Baixe este estudo de caso para aprender como uma agência do governo dos EUA, que teve um ataque parecido, está bloqueando os arquivos não autorizados. A lista da Bit 9 de aplicativos seguros tem como objetivo parar com esses tipos de ataque através das medidas:

- Impedindo que as DLLs sequestradas sejam executadas.
- Prevenindo a execução dos malwares (virus, cavalos-de-tróia etc.) desconhecidos.
- Verificando (validando) os arquivos DLL para saber se são autênticos e confiáveis.

Baixe o estudo de caso

Saudações,
Kate Munro
Bit 9 Incorporada

Baixe Agora

Imagem de relatório do "Centro de Desenvolvimento e de Pesquisa mantida pelo governo federal"

Resposta da Microsoft sobre esse novo ataque ao Windows

Microsoft Security Advisory (2269637)

Insecure Library Loading Could Allow Remote Code Execution
Published: August 23, 2010
Version: 1.0

http://www.microsoft.com/technet/security/advisory/2269637.mspx

General Information

Executive Summary

Microsoft is aware that research has been published detailing a remote attack vector for a class of vulnerabilities that affects how applications load external libraries.

This issue is caused by specific insecure programming practices that allow so-called "binary planting" or "DLL preloading attacks". These practices could allow an attacker to remotely execute arbitrary code in the context of the user running the vulnerable application when the user opens a file from an untrusted location.

This issue is caused by applications passing an insufficiently qualified path when loading an external library. Microsoft has issued guidance to developers in the MSDN article, Dynamic-Link Library Security, on how to correctly use the available application programming interfaces to prevent this class of vulnerability. Microsoft is also actively reaching out to third-party vendors through the Microsoft Vulnerability Research Program to inform them of the mitigations available in the operating sys-

tem. Microsoft is also actively investigating which of its own applications may be affected.

In addition to this guidance, Microsoft is releasing a tool that allows system administrators to mitigate the risk of this new attack vector by altering the library loading behavior system-wide or for specific applications. This advisory describes the functionality of this tool and other actions that customers can take to help protect their systems.

Mitigating Factors:

- This issue only affects applications that do not load external libraries securely. Microsoft has previously published guidelines for developers in the MSDN article, Dynamic-Link Library Security, that recommend alternate methods to load libraries that are safe against these attacks.
- For an attack to be successful, a user must visit an untrusted remote file system location or WebDAV share and open a document from this location that is then loaded by a vulnerable application.
- The file sharing protocol SMB is often disabled on the perimeter firewall. This limits the possible attack vectors for this vulnerability.

Advisory Details

Affected and Non-Affected Software

Microsoft is investigating whether any of its own applications are affected by insecure library loading vulnerabilities and will take appropriate action to protect its customers.

- Frequently Asked Questions
- Mitigating Factors and Suggested Actions
- Additional Suggested Actions

Other Information

Microsoft Active Protections Program (MAPP)

To improve security protections for customers, Microsoft provides vulnerability information to major security software providers in advance of each monthly security update release. Security software providers can then use this vulnerability information to provide updated protections to customers via their security software or devices, such as antivirus, network-based intrusion detection systems, or host-based intrusion prevention systems. To determine whether active protections are available from security software providers, please visit the active protections Web sites provided by program partners, listed in Microsoft Active Protections Program (MAPP) Partners.

Feedback

You can provide feedback by completing the Microsoft Help and Support

form, Customer Service Contact Us.

Support

- Customers in the United States and Canada can receive technical support from Security Support. For more information about available support options, see Microsoft Help and Support.
- International customers can receive support from their local Microsoft subsidiaries. For more information about how to contact Microsoft for international support issues, visit International Support.
- Microsoft TechNet Security provides additional information about security in Microsoft products.

Disclaimer

The information provided in this advisory is provided "as is" without warranty of any kind. Microsoft disclaims all warranties, either express or implied, including the warranties of merchantability and fitness for a particular purpose. In no event shall Microsoft Corporation or its suppliers be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages, even if Microsoft Corporation or its suppliers have been advised of the possibility of such damages. Some states do not allow the exclusion or limitation of liability for consequential or incidental damages so the foregoing limitation may not apply.

Revisions

V1.0 (August 23, 2010) Advisory published.