INDUSTRY TRENDS NETWORK SECURITY NEWS AND INSIGHTS

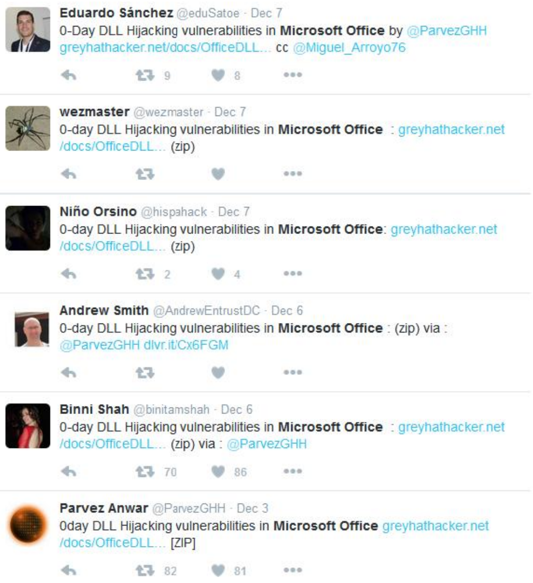
A Crash Course In DLL Hijacking

by Tien Phan (/author/tien-phan) | December 10, 2015 | Category: Industry Trends & News (/category/industry-trends-news)

690 1373 15 Google + 6

Overview

This week, we heard a lot about a DLL hijacking vulnerability from the security community. It began with a 0-day DLL hijacking in Microsoft Office which was discovered by independent security researcher named Parvez Anwar (https://twitter.com/parvezghh).



Eduardo Sánchez @eduSatoe · Dec 7
0-Day DLL Hijacking vulnerabilities in **Microsoft Office** by @ParvezGHH greyhathacker.net/docs/OfficeDLL… cc @Miguel_Arroyo76
9 8

wezmaster @wezmaster · Dec 7
0-day DLL Hijacking vulnerabilities in **Microsoft Office** : greyhathacker.net/docs/OfficeDLL… (zip)

Niño Orsino @hispahack · Dec 7
0-day DLL Hijacking vulnerabilities in **Microsoft Office**: greyhathacker.net/docs/OfficeDLL… (zip)
2 4

Andrew Smith @AndrewEntrustDC · Dec 6
0-day DLL Hijacking vulnerabilities in **Microsoft Office** : (zip) via : @ParvezGHH dlvr.it/Cx6FGM

Binni Shah @binitamshah · Dec 6
0-day DLL Hijacking vulnerabilities in **Microsoft Office** : greyhathacker.net/docs/OfficeDLL… (zip) via : @ParvezGHH
70 86

Parvez Anwar @ParvezGHH · Dec 3
0day DLL Hijacking vulnerabilities in **Microsoft Office** greyhathacker.net/docs/OfficeDLL… [ZIP]
82 81

Shortly after, the website securify.nl published an article (https://www.securify.nl/blog/SFY20151201/there_s_a_party_in_ole__and_you_are_invited.html) de this kind of attack and discussing the vast potential attack surface associated with DLLs and OLE.

A dynamic link library (DLL) is a basic component in the Windows operating system. Certain DLLs w loaded into Windows applications when they start if they are needed. DLLs provide software applica with resources such as Application Programming Interfaces (APIs) and additional procedures. If an a can control which DLL a program loads, then the attacker can insert a malicious DLL into the DLL lo process. In fact, this method is not new. Quite a few articles regarding this technique are available o Internet, especially from Microsoft (http://blogs.technet.com/b/srd/archive/2010/08/23/more-inform about-dll-preloading-remote-attack-vector.aspx).

In a nutshell, the vulnerability in this latest Microsoft 0-day lay in the way Microsoft Office searches fo components that are not present in the system, consequently allowing DLL hijacking attacks. But as detail below, that kind of vulnerability is not exclusive to Microsoft Office.

Attack Details

DLL search order is well documented by Microsoft (https://msdn.microsoft.com/en-us/library/ms682586%28v=vs.85%29.aspx). To recap, depending on the configuration of the system, a program can decide the order of the directories to be searched fo to load. By default, the order of this search is as follows:

1. The directory from which the application is loaded
2. The current directory
3. The system directory, usually C:\Windows\System32\ (The GetSystemDirectory function is called to obtain this directory.)
4. The 16-bit system directory - There is no dedicated function to retrieve the path of this directory, but it is searched as well.
5. The Windows directory. The GetWindowsDirector function is called to obtain this directory.
6. The directories that are listed in the PATH environment variable.

In this case, the current directory is the problem. When a program makes a decision to load a DLL from the current directory, it can lead to the DLL hijacking.

For example, if the user is opening a Microsoft Word document, Microsoft Office will try to load its DLL component from the location of that document file. An attacker can place a malicious DLL in the location of the document and as a result, Microsoft Office inadvertently loads the malicious code.

Another practical scenario is sharing a Microsoft Document file using Windows sharing with a malicious DLL (http://www.darkreading.com/risk-management/microsoft-pat dll-hijacking-vulnerability/d/d-id/1094065).

If SafeDllSearchMode is enabled, it is more difficult for an attacker to use this technique. In such a case, the DLL search order is as follows:

1. The directory specified by lpFileName function
2. The System directory (The GetSystemDirectory function is called to obtain this directory.)
3. The 16-bit system directory - There is no dedicated function to retrieve the path of this directory, but it is searched as well.
4. The Windows directory (The GetWindowsDirector y function is called to obtain this directory.)
5. The current directory
6. The directories that are listed in the PATH environment variable. Note that this does not include the per-application path specified by the App Paths registry key. The A Paths key is not used when computing the DLL search path.

Nonetheless, the current directory is still in the list of directories to be searched. The difference here is that the program searches system directories for a DLL component and, if not found, will then try the current directory.

How do I protect myself from DLL hijacking?

The following is some guidance to prevent you from becoming a victim of DLL-hijacking attacks.

For end users, the best way to prevent this attack is to apply the latest patch from the vendor. You can also harden your system using the following steps:

1. Open Notepad
2. Copy and paste the following text:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINESystemCurrentControlSetControlSession Manager]
"SafeDllSearchMode"=dword:00000001
[HKEY_LOCAL_MACHINESystemCurrentControlSetControlSession Manager]
"CWDIllegalInDllSearch"=dword:ffffffff
```

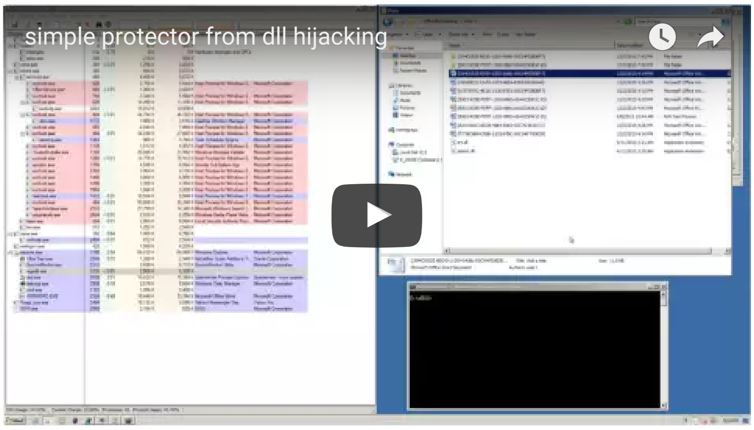
3. Save as “patch.reg” on your system.
4. Double click patch.reg and click Yes on the Windows prompt.

The above script will enable SafeDllSearchMode and disable loading of DLLs from the current directory.

For developers, you can follow the suggestions from Microsoft (http://blogs.technet.com/b/srd/archive/2010/08/23/more-information-about-dll-preloading-remote-attack-vector.aspx).

We also developed a small tool for learning and demonstration purposes. This tool will track new processes created. It will then apply a hook into any new process to forc to the *SetDLLDirectory* API with a blank argument. This means that any new process will be protected from loading DLLs located in the current directory. You can get the code of the tool here (https://github.com/fortiguard-lion/anti-dll-hijacking).

The following is a quick demo of the tool:



-= FortiGuard Lion Team =-

by **Tien Phan (/author/tien-phan)** | December 10, 2015 | Category: Industry Trends & News (/category/industry-trends-news)

690 1373 15 Google + 6

Tags: Microsoft OLE (/tag/microsoft-ole) | DLL (/tag/dll-1) | DLL Hijacking (/tag/dll-hijacking-1)

0 Comments Fortinet Blog 1 L

Recommend 2 Share Sort by

Start the discussion…

Be the first to comment.

Subscribe Add Disqus to your site Add Disqus Add Privacy DIS

FortiGuard Labs on the Web

Twitter (http://www.twitter.com/fortiguardlabs) Facebook (https://www.faceb

LinkedIn (http://www.linkedin.com/groups?gid=1321377&trk=hb_side_g) Youtube (http://www.youtub

Monthly Archives

November 2015 (/2015/11)	12
October 2015 (/2015/10)	19
September 2015 (/2015/09)	11
August 2015 (/2015/08)	17
July 2015 (/2015/07)	22
June 2015 (/2015/06)	18
May 2015 (/2015/05)	16
April 2015 (/2015/04)	34
March 2015 (/2015/03)	17
February 2015 (/2015/02)	11
January 2015 (/2015/01)	16
December 2014 (/2014/12)	7
November 2014 (/2014/11)	19
October 2014 (/2014/10)	16
September 2014 (/2014/09)	11
August 2014 (/2014/08)	11
July 2014 (/2014/07)	20
June 2014 (/2014/06)	21
May 2014 (/2014/05)	19
April 2014 (/2014/04)	16
March 2014 (/2014/03)	20
February 2014 (/2014/02)	15

January 2014 (/2014/01)	**25**
December 2013 (/2013/12)	**10**
November 2013 (/2013/11)	**15**
October 2013 (/2013/10)	**19**
September 2013 (/2013/09)	**19**
August 2013 (/2013/08)	**14**
July 2013 (/2013/07)	**14**
June 2013 (/2013/06)	**2**
April 2013 (/2013/04)	**1**
March 2013 (/2013/03)	**12**
February 2013 (/2013/02)	**11**
January 2013 (/2013/01)	**12**
December 2012 (/2012/12)	**8**
November 2012 (/2012/11)	**7**
October 2012 (/2012/10)	**4**
September 2012 (/2012/09)	**6**
August 2012 (/2012/08)	**7**
July 2012 (/2012/07)	**62**
June 2012 (/2012/06)	**17**
May 2012 (/2012/05)	**14**
April 2012 (/2012/04)	**15**
March 2012 (/2012/03)	**14**
February 2012 (/2012/02)	**11**
January 2012 (/2012/01)	**6**
December 2011 (/2011/12)	**4**
November 2011 (/2011/11)	**6**
October 2011 (/2011/10)	**11**
September 2011 (/2011/09)	**2**
August 2011 (/2011/08)	**2**
July 2011 (/2011/07)	**4**
June 2011 (/2011/06)	**6**
May 2011 (/2011/05)	**6**
April 2011 (/2011/04)	**5**
March 2011 (/2011/03)	**7**
February 2011 (/2011/02)	**5**
January 2011 (/2011/01)	**7**
December 2010 (/2010/12)	**8**
November 2010 (/2010/11)	**11**
October 2010 (/2010/10)	**3**
September 2010 (/2010/09)	**8**
August 2010 (/2010/08)	**4**
July 2010 (/2010/07)	**9**
June 2010 (/2010/06)	**9**

May 2010 (/2010/05)	**9**
April 2010 (/2010/04)	**6**
March 2010 (/2010/03)	**8**
February 2010 (/2010/02)	**6**
January 2010 (/2010/01)	**9**
December 2009 (/2009/12)	**8**
November 2009 (/2009/11)	**6**
October 2009 (/2009/10)	**6**
September 2009 (/2009/09)	**8**
August 2009 (/2009/08)	**5**
July 2009 (/2009/07)	**8**
June 2009 (/2009/06)	**7**
May 2009 (/2009/05)	**4**
April 2009 (/2009/04)	**7**
March 2009 (/2009/03)	**9**
February 2009 (/2009/02)	**4**
January 2009 (/2009/01)	**1**

Corporate

About Fortinet (http://fortinet.com/aboutus/aboutus.html)

Investor Relations (http://investor.fortinet.com/)

Careers (http://jobs.fortinet.com/)

Press Room (http://fortinet.com/press_releases/press.html)

Partners (http://fortinet.com/partners/index.html)

Global Offices (http://fortinet.com/aboutus/locations.html)

Fortinet Blog (http://blog.fortinet.com/)

Fortinet in the News (http://fortinet.com/aboutus/media/news.html)

Events (http://fortinet.com/events/index.html)

Contact Us (http://fortinet.com/contact_us/index.html)

How to Buy

Find a Reseller (http://fortinet.com/partners/reseller_locator/locator.html)

FortiPartner Program (http://fortinet.com/partners/partner_program/fpp.html)

Try & Buy (http://fortinet.com/how_to_buy/try_and_buy.html)

Fortinet Store (https://store.fortinet.com)

Products

Product Family (http://fortinet.com/products/index.html)

Certifications (http://fortinet.com/aboutus/fortinet_advantages/certifications.html)

Awards (http://fortinet.com/aboutus/fortinet_advantages/awards.html)

Video Library (http://video.fortinet.com/)

Service & Support

FortiCare Support (http://fortinet.com/support/forticare_support/index.html)

Support Helpdesk (https://support.fortinet.com/)

FortiGuard Center (http://fortiguard.com/)

Fortinet Blog (http://blog.fortinet.com)

(http://www.facebook.com/fortinet)

(http://www.twitter.com/fortinet)

(http://www.youtube.com/user/SecureNetworks)

(http://www.linkedin.com/company/fortinet)

(http://fortinet.com/rss.xml