

Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Statistiken Verletzbarkeiten
5. Labs
6. Bilderrätsel
7. Impressum

1. Editorial

Risikoanalysen und Resignation

Angewandte Computersicherheit stützt sich auf der Diskussion von Risikoanalysen ab. Es gilt die Bedrohungen zu erkennen. Danach wird die Eintrittswahrscheinlichkeit und die Auswirkungen skizziert, um die entsprechenden Risiken kalkulierbar zu machen.

Je eher ein Schaden Eintritt oder desto grösser seine Auswirkungen sind, desto grösser ist das Risiko. Und umso grösser das Risiko ist, desto eher lohnt es sich dagegen vorzugehen und will man es minimieren. Ein einfacher Prozess, eigentlich.

Teilweise wird jedoch aus diesem simplen Prinzip ein losgelöstes, realitätsfremdes und inkonsistentes Gebilde aufgebaut, welches sowohl die akademisch-juristischen Anforderungen der internen Revision als auch die praktisch-technischen Bedürfnisse der Administratoren nicht berücksichtigen kann.

Die Risikoanalysen finden meist auf Papier statt, ohne die detaillierten technischen Hintergründe der eingesetzten Produkte und Mechanismen zu kennen. Da wird dann halt pauschalisiert und versucht irgendwie zu allem ein Wort zu verlieren.

Die aus der Risikoanalyse generierten Massnahmenpakete adressieren sodann Probleme, die entweder so nie existiert haben

oder die sich auf einer ganz anderen Ebene und mit gänzlich unterschiedlichen Vorgehensweisen hätten beheben lassen.

Die Entwickler, Administratoren und Benutzer werden so sehr schnell "gegängelt". Wer Folge 2 der TV-Adaption von Dilbert gesehen hat, der weiss, wovon ich rede.

Die Konsequenz davon ist, dass Energie an Stellen verschwendet wird, die so gar nicht hätten berücksichtigt werden müssen. Sicherheit wird dann einmal mehr als nervige Mühsamkeit empfunden, die die Kreativität behindert und die Produktivität einschränkt. Und ja, in solchen Fällen kann man das nur schwerlich abstreiten.

Doch es ist nicht das Problem der Sicherheit oder der Risikoanalysen als solche. Viel mehr rührt der Fehler von einem unintelligenten Prozess. Oftmals zu spät und zu weit weg von der Realität werden die Risikoanalysen erstellt. Doch genau die Realität ist es, die man mit diesen Betrachtungen formalisieren und greifbar machen will.

Die Lösung kann nur sein, wenn die unterschiedlichen Stellen zusammenarbeiten und dadurch die unterschiedlichen Bedürfnisse in Einklang bringen lassen.

Einerseits die technischen Verantwortlichen, denen die technischen Details ihrer Lösungen bekannt sind. Andererseits die Verantwortlichen aus Information Security, deren Auftrag die Skizzierung und Adressierung von Risiken ist.

Das Erstellen einer Risikoanalyse und das Angehen der daraus resultierenden Massnahmen wird dann nicht mehr zu einer Bürde, sondern kann in den produktiven Prozess eingegliedert werden. Somit kann auch das eigentliche Ziel, die Gewährleistung der störungsfreien Geschäftsabwicklung eingehalten werden.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 18. Januar 2010

2. scip AG Informationen

2.1 Security Coaching

Das Ziel des Security Coaching ist die direkte Beratung und das unmittelbare Coaching des Kunden in den Bereichen der Information Security zur Sicherstellung nachhaltiger und sicherer Prozesse, Architektur- und Technologieentscheidungen.

Der Kunde bespricht mit uns seine Ziele und Vorgaben. Anhand dessen unterstützen wir den Kunden mit unserer fachmännischen Expertise und langjährigen Erfahrung im Security Bereich. Bei Sitzungen mit Partnern stellen wir das entsprechende Know-How zur Formulierung wichtiger Nachfragen zur Verfügung.

- Vorbereitung: Zusammentragen aller vorhandenen Informationen zur anstehenden Aufgabe.
- Research: Einholen von weiteren Informationen (z.B. Erfahrungen von anderen Kunden).
- Diskussion: Besprechung der Aufgabe und der daraus resultierenden Möglichkeiten.
- Empfehlung: Aussprechen und Dokumentieren eines vertretbaren Lösungswegs.

In erster Linie soll in beratender Weise eine direkte Hilfestellung mit konkreten Empfehlungen und Lösungen bereitgestellt werden. Eine Dokumentation (Protokolle, Kommunikationsmatrizen, Statements etc.) erfolgt auf Wunsch des Kunden.

Durch die direkte Beteiligung an einem Projekt kann unmittelbar Einfluss ausgeübt, damit die Etablierung schwerwiegender Fehler verhindert und ein Höchstmass an Sicherheit erreicht werden. Da Sicherheit von Beginn an zur Diskussion steht, lassen sich Schwachstellen von vornherein vermeiden. Aufwendigen Tests und nachträgliche Anpassungen können so vorgebeugt werden.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen konnten wir als scip AG bereits eine grosse Anzahl an Kunden beraten und begleiten.

Zählen auch Sie auf uns!

<http://www.scip.ch/?firma.referenzenalle>

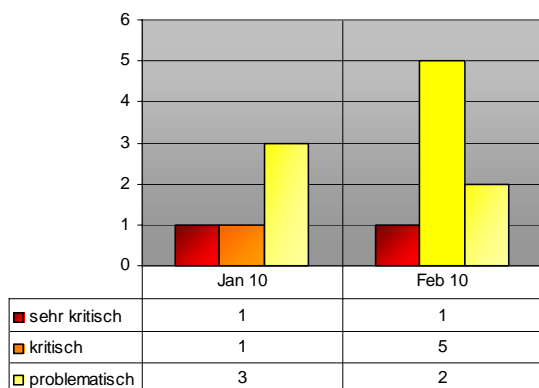
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch.

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/?vuldb> einsehbar.



Die Dienstleistungspakete scip(pallas liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.



Contents:

- 4087 Microsoft DirectShow AVI File Parsing Pufferüberlauf
- 4086 Microsoft Windows CSRSS Privilege Escalation Schwachstelle
- 4085 Microsoft Windows SMB Client Implementation Schwachstellen
- 4084 Microsoft Windows Shell Handler Input Validation Schwachstelle
- 4083 Microsoft Windows Paint JPEG Parsing Integer Overflow
- 4082 Microsoft Office PowerPoint verschiedene Schwachstellen
- 4081 Trend Micro OfficeScan URL Filtering Engine Pufferüberlauf
- 4080 Microsoft Internet Explorer Local File Disclosure

3.1 Microsoft DirectShow AVI File Parsing Pufferüberlauf

Risiko: **sehr kritisch**

Remote: Ja

Datum: 09.02.2010

scip DB: <http://www.scip.ch/?vuldb.4087>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser

Entwicklungszeit zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. In einem Advisory beschreibt der Hersteller eine Schwachstelle in verschiedenen Windows Versionen, bei denen beliebiger Code mittels eines Pufferüberlauf Fehlers beim Bearbeiten von AVI Daten via DirectShow zur Ausführung gebracht werden kann.

Expertenmeinung:

Erneut stellt DirectShow einen nützlichen Angriffspunkt für sehr potente Exploits dar. Es ist zu erwarten, dass die vorliegende Schwachstelle zeitnah flächendeckend ausgenutzt werden kann. Die vorliegende Schwachstelle somit ist als kritisch zu betrachten und sollte zeitnah durch das Einspielen des entsprechenden Patches adressiert werden.

3.2 Microsoft Windows CSRSS Privilege Escalation Schwachstelle

Risiko: **problematisch**

Remote: Ja

Datum: 09.02.2010

scip DB: <http://www.scip.ch/?vuldb.4086>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszeit zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Mathew Jurczyk identifizierte eine Schwachstelle, bei der ein Angreifer seine Rechte durch das Ausnutzen einer Schwachstelle im CSRSS Dienst erweitern kann. Microsoft hat zu dieser Schwachstelle in Form eines Security Bulletins Stellung genommen.

Expertenmeinung:

Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah durch das Einspielen des entsprechenden Patches adressiert werden.

3.3 Microsoft Windows SMB Client Implementation Schwachstellen

Risiko: **problematisch**

Remote: Ja

Datum: 09.02.2010

scip DB: <http://www.scip.ch/?vuldb.4085>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft.

Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Laurent Gaffié beschreibt in einem Advisory zahlreiche Schwachstellen in der Implementation des SMB Clients in verschiedenen Windows Versionen, die von einem Angreifer zur Eskalation seiner Privilegien ausgenutzt werden können. Microsoft hat zu diesen Schwachstellen in Form eines Security Bulletins Stellung genommen.

Expertenmeinung:

Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah durch das Einspielen des entsprechenden Patches adressiert werden.

3.4 Microsoft Windows Shell Handler Input Validation Schwachstelle

Risiko: **kritisch**

Remote: Ja

Datum: 09.02.2010

scip DB: <http://www.scip.ch/?vuldb.4084>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Brett Moore identifizierte eine Schwachstelle in verschiedenen Windows Versionen, bei denen Angreifer durch einen Input Validation Fehler im Shell Handler beliebigen Code zur Ausführung bringen können.

Expertenmeinung:

Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah durch das Einspielen des entsprechenden Patches adressiert werden.

3.5 Microsoft Windows Paint JPEG Parsing Integer Overflow

Risiko: **kritisch**

Remote: Ja

Datum: 09.02.2010

scip DB: <http://www.scip.ch/?vuldb.4083>

Microsoft Windows ist ein Markenname für

Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Tielei Wang identifizierte eine Integer Overflow Lücke in Microsoft's eigenem Zeichnungs-Tool "Paint", bei der durch das Parsing von entsprechend präparierten JPEG Bilddateien beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:

Eine kritische Schwachstelle in einer der klassischsten und wohlbekanntesten, aber gleichzeitig auch trivialsten Applikationen von Windows zu schreiben könnte einem zu so mancher lakonischen Äusserung verleiten. Dennoch sei an dieser Stelle angemerkt, dass die vorliegende Schwachstelle dazu genutzt werden kann, Systeme zu kompromittieren und daher zeitnah gepatcht werden sollte.

3.6 Microsoft Office PowerPoint verschiedene Schwachstellen

Risiko: **kritisch**

Remote: Ja

Datum: 09.02.2010

scip DB: <http://www.scip.ch/?vuldb.4082>

Microsoft PowerPoint ist ein Computerprogramm, mit dem sich interaktive Präsentationen unter Windows und Mac OS erstellen lassen. PowerPoint ist das am weitesten verbreitete Präsentationsprogramm. Nach Schätzungen von Microsoft werden damit täglich rund 30 Millionen Präsentationen erstellt. Verschiedener Researcher weisen auf Schwachstellen in Microsoft Powerpoint hin, unter deren Ausnutzung ein Angreifer beliebigen Code auf dem Zielsystem zur Ausführung bringen kann. Microsoft reagiert dieser Tage darauf mit einem Security Bulletin und einem Patch, der diese Schwächen schliessen soll.

Expertenmeinung:

Diverse Schwachstellen kritischer Natur werden im vorliegenden Bulletin besprochen, die mit hoher Wahrscheinlichkeit zeitnah durch Angreifer ausgenutzt werden. Administratoren wie Anwender zugleich sollten daher um eine zeitnahe Einspielung innerhalb der ihnen anvertrauten Infrastruktur bemüht sein.

3.7 Trend Micro OfficeScan URL

Filtering Engine Pufferüberlauf

Risiko: **kritisch**

Remote: Ja

Datum: 04.02.2010

scip DB: <http://www.scip.ch/?vuldb.4081>

Das japanische Unternehmen Trend Micro Incorporated (jap. トレンドマイクロ株式会社, torendo maikuro kabushiki-gaisha), gelistet im Nikkei 225, ISIN JP3637300009, ist ein weltweit agierender Anbieter von Software und Dienstleistungen in den Bereichen Virenschutz für Netzwerke, Anti-Spam und Internet Content Security. Der Hersteller weist in einem Advisory auf eine Schwachstelle in seinem Produkt OfficeScan hin, durch die ein Angreifer einen Pufferüberlauf auf dem System verursachen kann, was zu dessen Kompromittierung führen kann.

Expertenmeinung:

Administratoren des besagten Produktes sollten zeitnah den erscheinenden Patch zum Einsatz bringen, um einer längerfristige Exponierung zu vermeiden.

3.8 Microsoft Internet Explorer Local File Disclosure

Risiko: **problematisch**

Remote: Ja

Datum: 04.02.2010

scip DB: <http://www.scip.ch/?vuldb.4080>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Im Betriebssystem-eigenen Browser Internet Explorer existieren gemäss eines aktuellen Advisories verschiedene Schwachstelle, unter deren Nutzung die Existenz lokaler Files nachgewiesen werden kann.

Expertenmeinung:

Die vorliegende Schwachstelle ist nicht als kritisch zu betrachten, sollte aber dennoch bewusst wahrgenommen werden. Die Verfasser des Advisories weisen darauf hin, dass die Aktivierung des Protocol Lockdowns in Windows XP das Problem zumindest vordergründig zu lösen vermag.

4. Statistiken Verletzbarkeiten

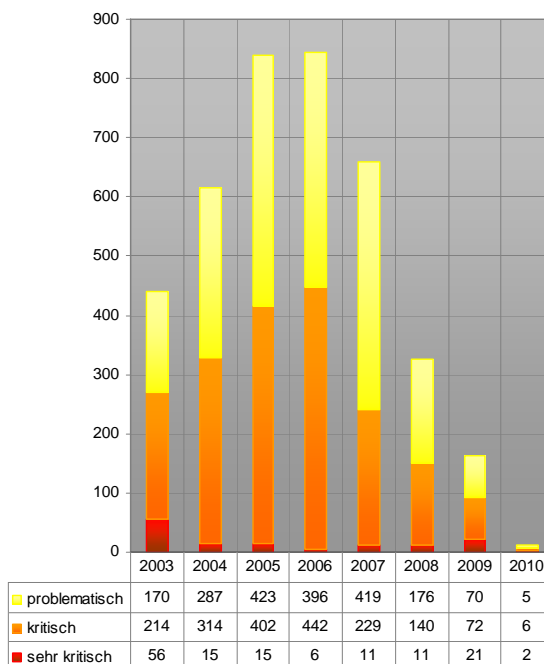
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



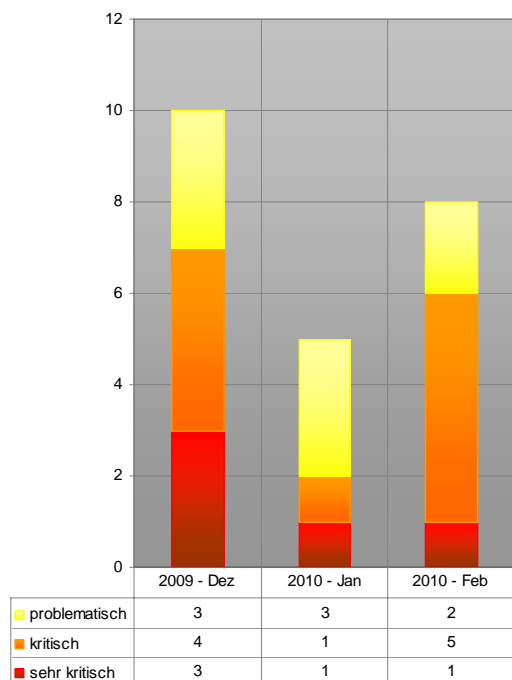
<http://www.scip.ch/?vuldb>

Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

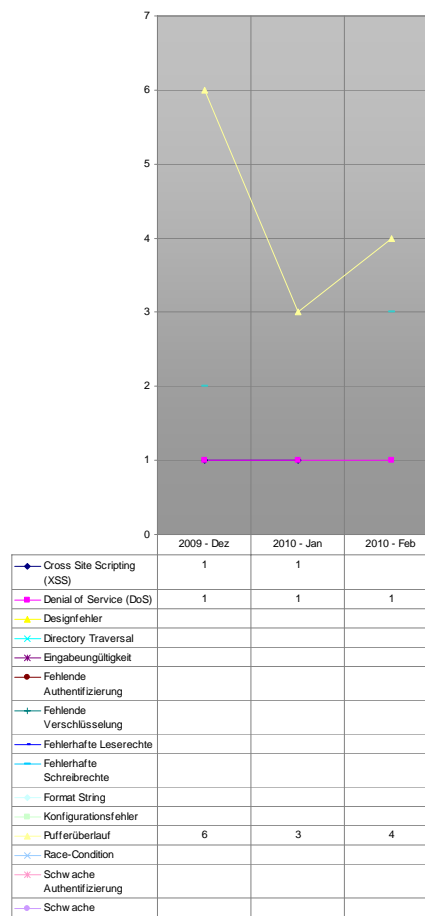
Auswertungsdatum: 19. Februar 2010



Verlauf der Anzahl Schwachstellen pro Jahr

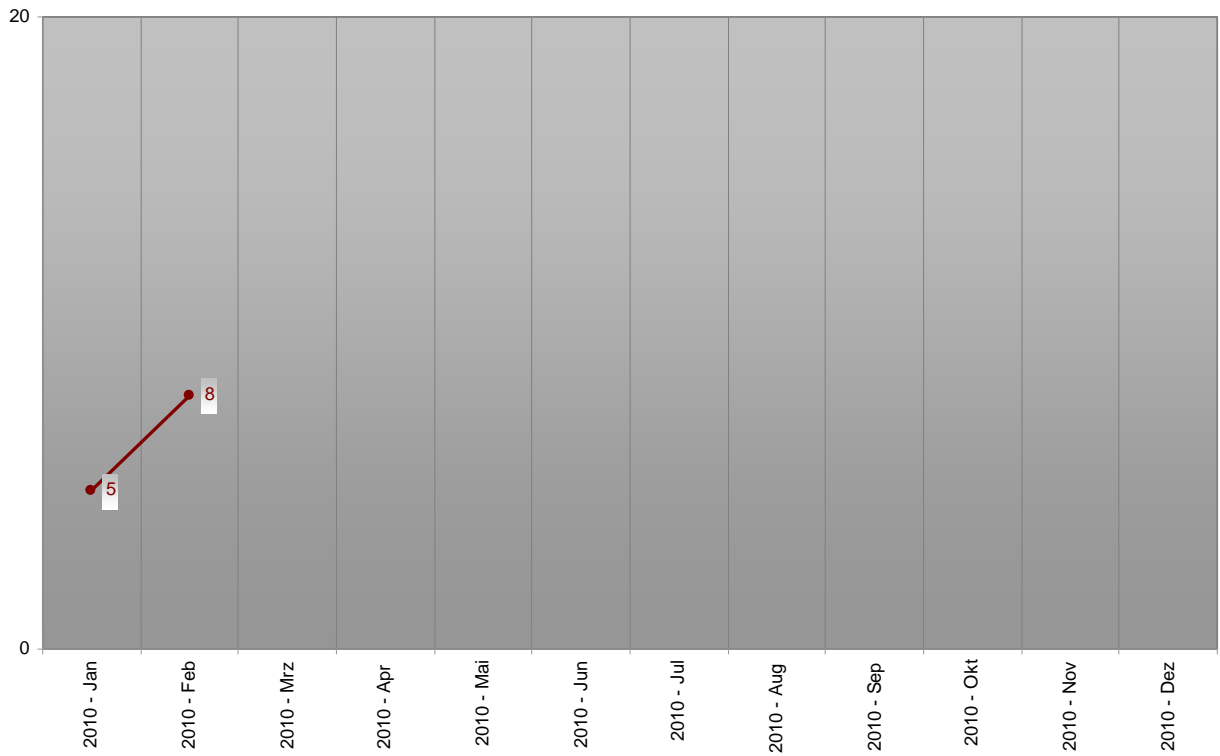


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

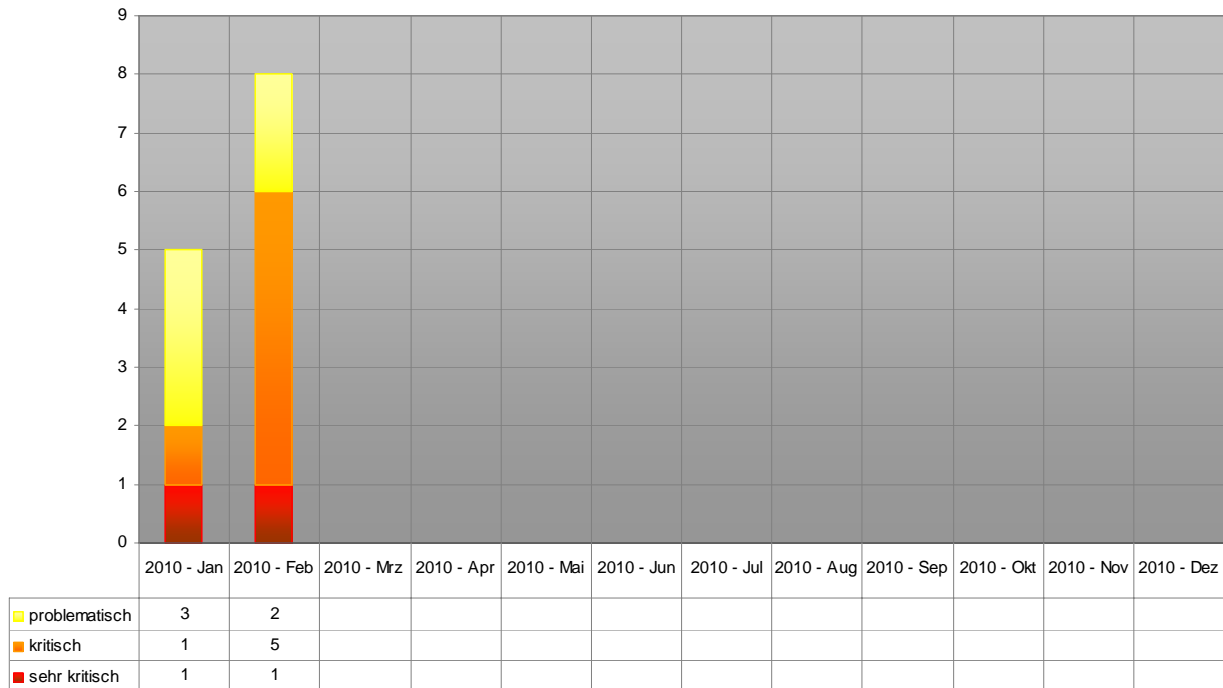


Verlauf der letzten drei Monate Schwachstelle/Kategorie

Registrierte Schwachstellen by scip AG



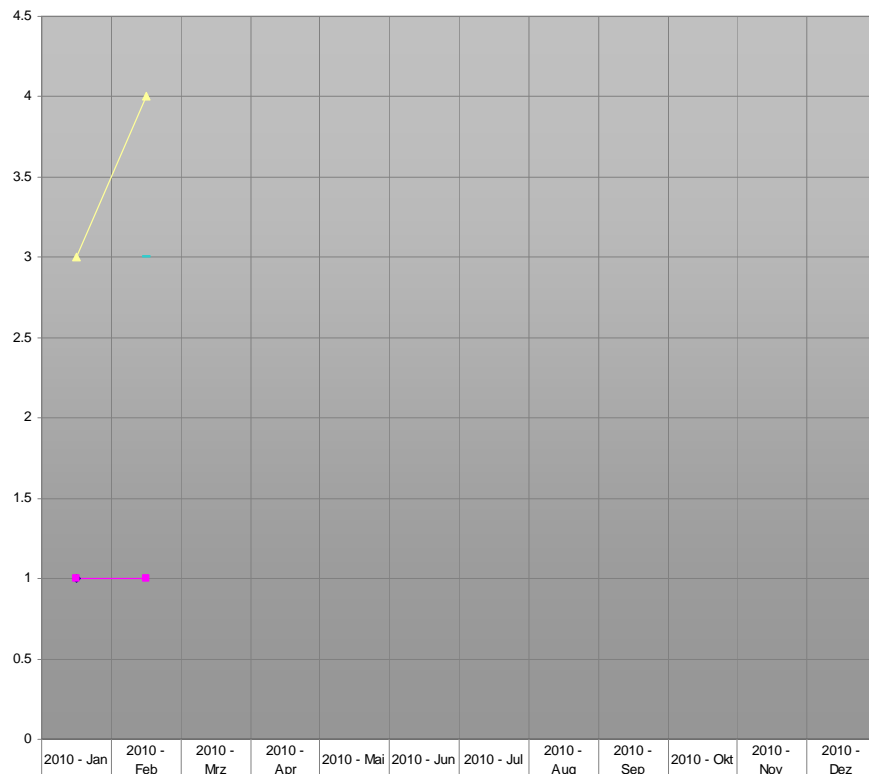
Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2010



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2010

scip monthly Security Summary 19.02.2010

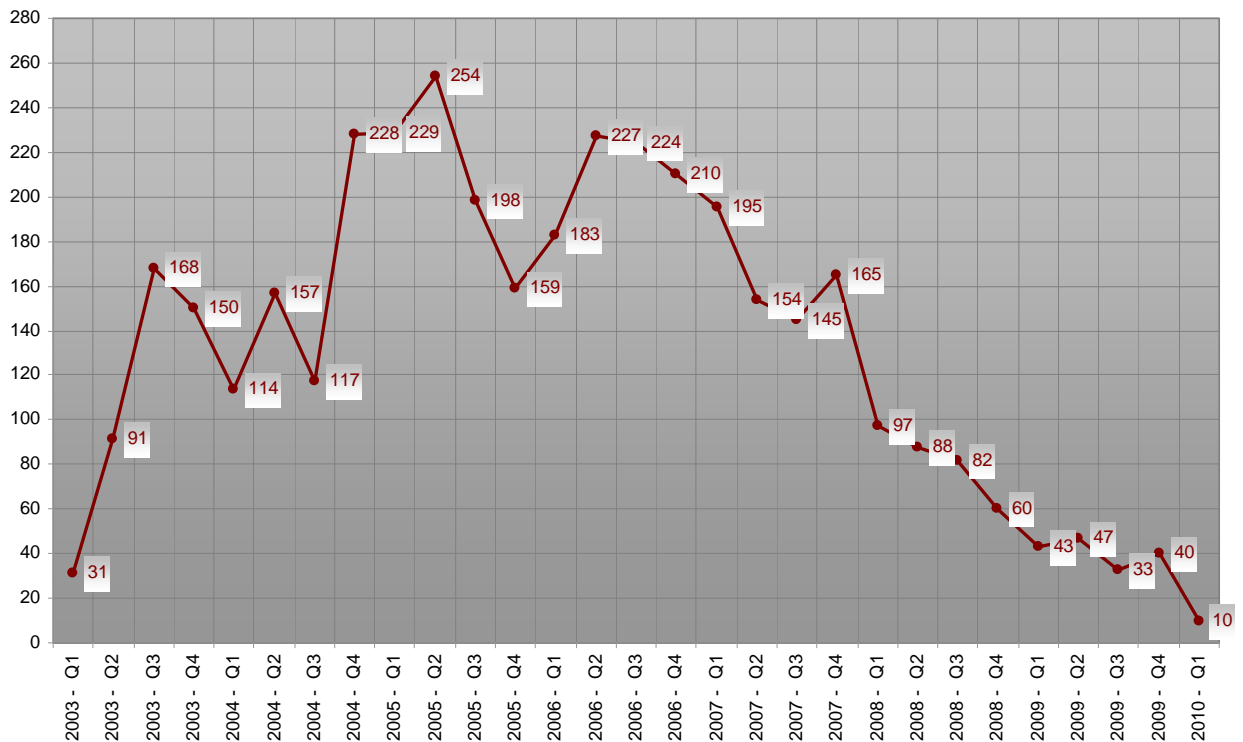




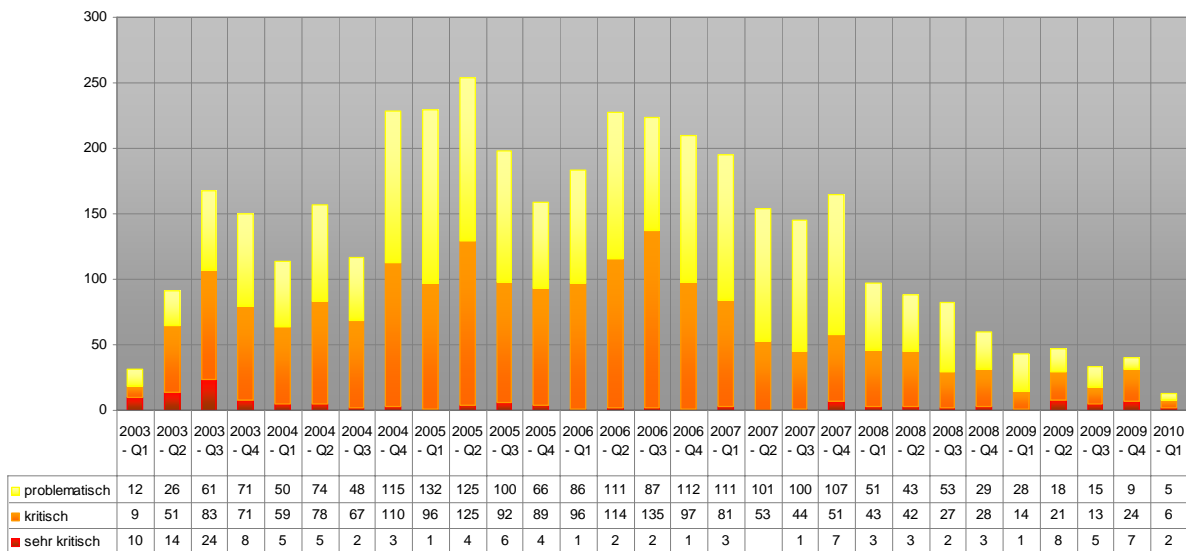
	2010 - Jan	2010 - Feb	2010 - Mrz	2010 - Apr	2010 - Mai	2010 - Jun	2010 - Jul	2010 - Aug	2010 - Sep	2010 - Okt	2010 - Nov	2010 - Dez
◆ Cross Site Scripting (XSS)	1											
◆ Denial of Service (DoS)	1	1										
◆ Designfehler												
◆ Directory Traversal												
◆ Eingabeungültigkeit												
◆ Fehlende Authentifizierung												
◆ Fehlende Verschlüsselung												
◆ Fehlerhafte Leserechte												
◆ Fehlerhafte Schreibrechte												
◆ Format String												
◆ Konfigurationsfehler												
◆ Pufferüberlauf	3	4										
◆ Race-Condition												
◆ Schwache Authentifizierung												
◆ Schwache Verschlüsselung												
◆ SQL-Injection												
◆ Symink-Schwachstelle												
◆ Umgehungs-Angriff		3										
◆ Unbekannt												

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2010

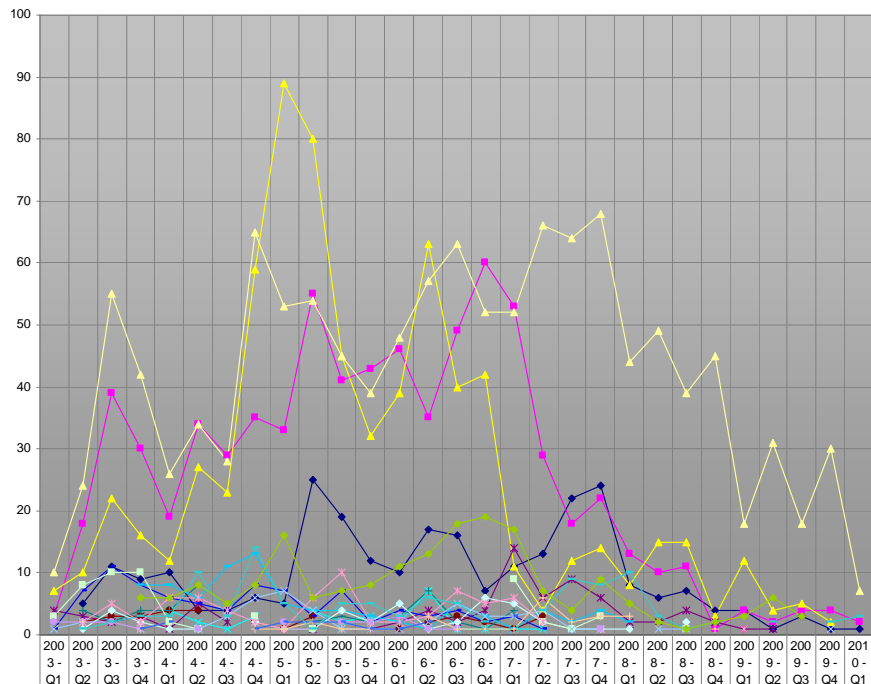
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Quartal seit 2003 Q1



Verlauf der Anzahl Schwachstellen/Schweregrad pro Quartal seit 2003 Q1



	2003-Q1	2003-Q2	2003-Q3	2003-Q4	2004-Q1	2004-Q2	2004-Q3	2004-Q4	2005-Q1	2005-Q2	2005-Q3	2005-Q4	2006-Q1	2006-Q2	2006-Q3	2006-Q4	2007-Q1	2007-Q2	2007-Q3	2007-Q4	2008-Q1	2008-Q2	2008-Q3	2008-Q4	2009-Q1	2009-Q2	2009-Q3	2009-Q4	2010-Q1	
◆ Cross Site Scripting (XSS)		5	11	9	10	4	4	6	5	25	19	12	10	17	16	7	11	13	22	24	8	6	7	4	4	1	3	1	1	
◆ Denial of Service (DoS)	3	18	39	30	19	34	29	35	33	55	41	43	46	35	49	60	53	29	18	22	13	10	11	1	4	2	4	4	2	
◆ Designfehler	7	10	22	16	12	27	23	59	89	80	45	32	39	63	40	42	11	4	12	14	8	15	15	3	12	4	5	2		
◆ Directory Traversal					4	2	1	3	4	2	3	2	7	1	1	1	1													
◆ Eingabeungültigkeit	4	3	2	3	1	5	2		1	1			1	2	4	2	4	14	6	9	6	2	2	4	2	1	1			
◆ Fehlende Authentifizierung		2	3	3	4	4		2	1	3				1	2	3	2	1	3											
◆ Fehlende Verschlüsselung		4	2	4	4	8				2	3	2	3	7	2	1	4													
◆ Fehlerhafte Leserechte	1	7	11	8	6	5	4	8	7	3	7	2	4	3	4	2	3	1				1								
◆ Fehlerhafte Schreibrechte				8	8	6	11	13	5	4	4	3	2	1	5	3	1	4	2	4	2									
◆ Format String		1	4	2	1	1		2	1	1	4	2	5	1	2	6	5	2	1	1	1		2							
◆ Konfigurationsfehler	3	8	10	10	2	1		3	1								9	2	1	3										
◆ Pufferüberlauf	10	24	55	42	26	34	28	65	53	54	45	39	48	57	63	52	52	66	64	68	44	49	39	45	18	31	18	30	7	
◆ Race-Condition	1	2		1	1	3	6	7	4	1	1	1	2	5	3	3	4	1	1			1	1						1	
◆ Schwache Authentifizierung		2	5	2	6	6	4	2	1	6	10	2	2	3	7	5	6	2		1							1			
◆ Schwache Verschlüsselung	2	2	2	1		1			2		2	2	3	1	1					1										
◆ SQL-Injection		2		1			1	1	2	1	1		3	1	1	1	6	2	3	3				1						
◆ Symink-Schwachstelle				1	2			1	2	2	1	1	2				3													
◆ Umgehungs-Angriff	1	2	3	3	10	3	14	5	1	5	5	3	6	5	2		4	9	8	10	3	1	2			2		2	3	
◆ Unbekannt				6	6	8	5	8	16	6	7	8	11	13	18	19	17	7	4	9	5	2	1	2	3	6	3			

Verlauf der Anzahl Schwachstellen/Kategorie pro Quartal seit 2003 Q1

5. Labs

Auf der scip Labs Webseite (<http://www.scip.ch/?labs.archiv>) werden regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

5.1 Aurora - Anatomie einer medienwirksamen Schwachstelle

05.02.2010 Marc Ruef, maru@scip.ch

Der Bereich der Computersicherheit fristet ein gewisses Schattendasein. Nur sehr selten werden Entwicklungen von der breiten Öffentlichkeit wahrgenommen. Nur manchmal gibt es Sicherheitslücken, Malware oder Angriffe, die es in die Tagesmedien schaffen. Die ersten medienwirksamen Meldungen wurden durch Würmer wie Melissa und ILOVEYOU sowie die ersten grossflächigen Distributed Denial of Service-Attacken (DDoS) gegen eBay und Yahoo generiert.



12.01.2010 – Der Zwischenfall

Die letzten Jahre haben keine grösseren Meldungen hervorgebracht. Dafür ist im Januar dieses Jahres der Zwischenfall, der unter dem Namen Aurora bekannt werden sollte, umso mehr eingeschlagen. Den Stein ins Rollen brachte die Meldung von Google, in der darauf hingewiesen wird, dass Google selbst im Dezember des vergangenen Jahres Opfer eines Hacker-Angriffs wurde. Bei diesem Zwischenfall seien zielgerichtet urheberrechtlich geschützte Inhalte (Quelltexte) gestohlen sowie Zugriffe auf Gmail-Konten von chinesischen Menschenrechtsaktivisten durchgesetzt worden. Da die ersten Untersuchungen gezeigt hatten, dass bei den Angriffen die chinesische Regierung federführend gewesen war, wolle man sich aus Protest – ebenfalls gegenüber den auferlegten Zensurmassnahmen – aus dem chinesischen Markt zurückziehen:

These attacks and the surveillance they have uncovered—combined with the attempts over the past year to further limit free speech on the web—have led us to conclude that we should review the feasibility of our business operations in China. We have decided we are no longer willing to continue censoring our re-

sults on Google.cn, and so over the next few weeks we will be discussing with the Chinese government the basis on which we could operate an unfiltered search engine within the law, if at all. We recognize that this may well mean having to shut down Google.cn, and potentially our offices in China.

Die Tagesmedien verbreiten diese Meldung, obschon sich dabei in erster Linie auf wirtschaftliche und politische Aspekte dieses schwelenden Konflikts fokussiert wird. Das Problem des Datendiebstahls wird zwar erwähnt, geniesst jedoch kein besonders hohes (technisches) Interesse.

14.01.2010 – Internet Explorer als Einfallstor
Schon bald wurden erste Gerüchte laut, dass eine Schwachstelle im Adobe Reader ausgenutzt wurde, um erweiterte Zugriffsrechte zu erlangen. Konkrete technische Details oder eine verlässliche Quelle wurden hierfür jedoch nicht genannt. Weitere Firmen, darunter auch Adobe selbst, bestätigten, dass auch sie Opfer derartiger Angriffe wurden.

Zwei Tage nach dem Bekanntwerden der Angriffe auf Google und andere namhafte Firmen in China, veröffentlichte Microsoft das Microsoft Security Advisory 979352. Dieses beschreibt eine kritische Schwachstelle im Internet Explorer, durch den erweiterte Rechte erlangt werden können (CVE-2010-0249):

The vulnerability exists as an invalid pointer reference within Internet Explorer. It is possible under certain conditions for the invalid pointer to be accessed after an object is deleted. In a specially-crafted attack, in attempting to access a freed object, Internet Explorer can be caused to allow remote code execution.

Da Microsoft die Beteiligung von Google an diesem Advisory zuspricht, werden erste Vermutungen geäussert, dass anstatt des unbekanntes PDF-Exploit eben diese Schwachstelle im Internet Explorer für die Einbrüche genutzt werden hätten können.

Das technische Interesse am Exploit steigt sprunghaft an. Und so wird auf wepawet.iseclab.org ein funktionierender, in Javascript geschriebener Exploit veröffentlicht. Einen Tag später wird dieser in das MetaSploit Framework (MSF) integriert und im hauseigenen Blog angekündigt:

Yesterday, a copy of the unpatched Internet Explorer exploit used in the Aurora attacks was uploaded to Wepawet. Since the code is now public, we ported this to a Metasploit

module in order to provide a safe way to test your workarounds and mitigation efforts.

Die Tagesmedien beginnen die Tragweite der genutzten Angriffsmöglichkeit zu verstehen. Nachdem in den ersten Meldungen auf die Nennung der technischen Hintergründe verzichtet wurde, rückt von nun an der Internet Explorer als Corpus Delicti in den Mittelpunkt des Interesses.

15.01.2010 – Warnung vor dem Internet Explorer In vollkommene Ungnade fällt der Browser von Microsoft, als das BSI (Bundesamt für Sicherheit in der Informationstechnik) eine öffentliche Warnung vor dessen Einsatz ausspricht:

Das Ausführen des Internet Explorer im „geschützten Modus“ sowie das Abschalten von Active Scripting erschwert zwar die Angriffe, kann sie jedoch nicht vollständig verhindern. Deshalb empfiehlt das BSI, bis zum Vorliegen einer Patches von Microsoft auf einen alternativen Browser umzusteigen.

Die französische CERTA (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques) zieht nach und spricht ebenfalls die Empfehlung aus, einen alternativen Browser einzusetzen:

Dans l'attente d'un correctif de l'éditeur, Le CERTA recommande l'utilisation d'un navigateur alternatif.

18.01.2010 – Weiterführende Entwicklungen Microsoft hat mittlerweile bemerkt, dass ihnen die Berichterstattungen rund um den Aurora-Zwischenfall nicht zu gute kommen. In verschiedenen Nachrichtenmagazinen dementiert Microsoft, dass der Einsatz des Internet Explorer mit einem erhöhten Risiko verbunden ist.

Das Sicherheitsunternehmen VUPEN stellt mittlerweile ihren bezahlenden Kunden eine modifizierte Version des Exploits zur Verfügung, der einen DEP-Bypass umsetzen kann. Die Empfehlung, die Data Execution Prevention einzuschalten, kann also spätestens jetzt nicht mehr vor dem Ausnutzen der Schwachstelle bewahren:

This remote code execution exploit with DEP (Data Execution Prevention) bypass takes advantage of a use-after-free vulnerability in Microsoft Internet Explorer when handling certain event objects.

Und wahrhaftig scheint die Angst vor dem Internet Explorer sprunghaft gewachsen zu sein. So vermelden die Mozilla-Entwickler in einem Blog-Post, dass der Download des Firefox seit der Warnung des BSI markant angestiegen ist. Vor allem Benutzer aus Deutschland scheinen sich

für die vermeintlich sicherere Alternative zu interessieren:

Looking at the chart below, we can see that over the past few days there has been a huge increase in the number of Firefox downloads from IE users in Germany. The orange area is meant to represent the “incremental” impact, i.e., the number of downloads beyond what we would have normally expected on those days. As the chart highlights, the orange area adds up to just over 300,000 downloads during the recent Friday-Monday period.

Microsoft kündigt am 20.01.2010 einen ausserplanmässigen Patch an. Dieser soll morgen erscheinen und die viel diskutierte Schwachstelle im Internet Explorer beheben:

This is an advance notification of one out-of-band security bulletin that Microsoft is intending to release on January 21, 2010. The bulletin will be for Internet Explorer to address limited attacks against customers of Internet Explorer 6, (...)

Dieser erscheint dann auch wie erwartet und wird natürlich vielerorts unverzüglich eingespielt. Die Gefahr schien damit vorerst gebannt zu sein. Genau rechtzeitig, denn mittlerweile ist eine breitflächige Ausnutzung der viel besprochenen Schwachstelle zu beobachten.

24.01.2010 – China dementiert China hatte sich zu den Anschuldigungen von Seiten Google stets bedeckt gehalten. Die Involvierung in den Cyberangriffen wurde anfangs weder dementiert noch bestätigt. Die Regierung hat sich sodann doch nicht durchgerungen, sich dahingehend zu äussern und eine Beteiligung vehement zu verneinen:

China on Friday firmly dismissed accusations by the United States that Beijing restricts Internet freedom and warned such claims were damaging to relations between the two nations.

Verschiedene technische Portale beginnen sich nun zu fragen, ob und inwiefern die Patch-Policy von Microsoft Mitschuld daran trägt, dass ein solcher Angriff überhaupt stattfinden konnte. Joe Stewart setzte eine umfassende Analyse der eingesetzten Exploits um und kam zum Schluss, dass das Problem wohl schon seit etwa 4 Jahren Microsoft bekannt gewesen wird. Denn so seien einige Codeteile schon 2006 geschrieben worden:

It appears that development of Aurora has been in the works for quite some time – some of the custom modules in the Aurora code-

base have compiler timestamps dating back to May 2006.

Doch nicht alle glauben daran, dass nicht zwingend China hinter den Attacken steckt. Und wer sich ein bisschen mit den Methoden krimineller Aktivitäten im Cyberspace auskennt, der weiss, dass China sehr gerne als Zwischenstation missbraucht wird. Zwar äussert sich China offen dazu, in dieser Hinsicht Bestrebungen voranzutreiben. Jedoch einen derartig umfassenden Angriff in derartig offensichtlicher Weise aus dem eigenen Land zu starten, passt so gar nicht in das Schema einer wohl vorbereiteten Attacke.

Fazit

Im Informationszeitalter ist Computersicherheit nicht mehr wegzudenken. Das Verständnis für bestehende Gefahren und laufende Entwicklungen hilft der Gesellschaft, mit den Risiken der heutigen Zeit umzugehen. Dass ausgerechnet die Schwachstelle im Internet Explorer von solcher Medienwirksamkeit gelangte, ist aus technischer Sicht nur bedingt nachzuvollziehen. Die Schwachstelle ist weder technisch noch wirtschaftlich besonders interessant.

Es gibt zudem eine Vielzahl an Sicherheitslücken im Internet Explorer, die eine vergleichbare technische Tragweite haben und auch noch immer nicht gepatcht sind (wahrscheinlich, weil sie offiziell noch nicht ausgenutzt wurden). Dass die Tagesmedien von nun an über jeden 0-Day in einem populären Produkt berichten, ist der Sache auch nicht dienlich.

Des Weiteren ist die allgemeine Empfehlung des BSI, auf den Internet Explorer zu verzichten, keine echte Lösung. Eine statistische Auswertung der im Mozilla Firefox in den letzten Jahren gemeldeten Schwachstellen zeigt auf, dass dieser nicht viel sicherer ist. Im Gegensatz zu Microsoft ist das Mozilla-Team jedoch stets darum bemüht, kritische Fehler schnellstmöglich zu beheben, weshalb das Zeitfenster für erfolgreiche Angriffe minimiert werden kann. Microsoft täte gut daran, (vermeintliche) Schwachstellen auch dann zu beheben, wenn es noch keine funktionierenden Exploits gibt. Denn spätestens dann, wenn ein solcher bekannt wird, ist es definitiv zu spät.

Links:

<http://blog.fefe.de/?ts=b5a024a3>

<http://blog.metasploit.com/2010/01/reproducing-aurora-ie-exploit.html>

<http://blog.mozilla.com/metrics/2010/01/19/people-in-germany-are-switching-browsers/>

<http://blog.osvdb.org/2010/01/24/microsoft-aurora-and-something-about-forest-and-trees>

http://blogs.adobe.com/conversations/2010/01/adobe_investi_gates_corporate_n.html

<http://blogs.technet.com/msrc/archive/2010/01/21/bulletin-ms10-002-released.aspx>

<http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0249>

<http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>

http://news.xinhuanet.com/english2010/china/2010-01/24/c_13148845.htm

<http://taosecurity.blogspot.com/2010/01/google-v-china.html>

<http://techblog.avira.com/2010/01/15/security-hole-in-internet-explorer-gets-exploited/en/>

http://threatpost.com/en_us/blogs/aurora-attack-malware-components-may-be-four-years-old-012010

<http://twitter.com/VUPEN/status/7942550681>

<http://wepawet.iseclab.org/view.php?hash=1aea206aa64e4ebb07237f1e2230d0f&type=is>

<http://www.certa.ssi.gouv.fr/site/CERTA-2010-ALE-001/CERTA-2010-ALE-001.html>

<http://www.computec.ch/news.php?item.310>

http://www.csoonline.com/article/515777/Hackers_Used_Rigged_PDFs_to_Hit_Google_and_Adobe

<http://www.itworld.com/security/93670/widespread-attacks-exploit-newly-patched-ie-bug>

<http://www.microsoft.com/technet/security/advisory/979352.mspx>

<http://www.microsoft.com/technet/security/bulletin/ms10-ian.mspx>

<http://www.secureworks.com/research/blog/index.php/2010/01/20/operation-aurora-clues-in-the-code/>

<http://www.sophos.com/blogs/gc/g/2010/01/22/prove-china-operation-aurora/>

<http://www.symantec.com/connect/blogs/trojanhydraq-incident-analysis-aurora-0-day-exploit>

<http://www.tagesschau.de/inland/internetexplorer102.html>

<http://www.tagesschau.de/wirtschaft/google206.html>

<http://www.techradar.com/news/internet/microsoft-switch-from-ie-and-your-risk-increases-664429>

http://www.theregister.co.uk/2010/01/26/aurora_attack_origin/

http://www.uscc.gov/researchpapers/2009/NorthropGrumman_PRC_Cyber_Paper_FINAL_Approved%20Report_16Oct2009.pdf

http://www.vupen.com/exploits/Microsoft_Internet_Explorer_Use_after_free_Code_Execution_Exploit_MS_979352_0135286.php

https://www.bsi.bund.de/clin_174/ContentBSI/presse/Pressemittellungen/Sicherheitsluecke_IE_150110.html

6. Bilderrätsel



GESUCHTE BEGRIFFE

4 (english)	9 (english)	10 (english)

LÖSUNGSWORT

Wettbewerb

Mailen Sie uns das erarbeitete Lösungswort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten. Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.03.2010**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung des Bilderrätsel finden Sie jeweils online auf <http://www.scip.ch>.

Gewinnen Sie einen Monat des [Securitytracker](#) Dienstes [\)pallas\(](#).

SECURITYTRACKER



7. Impressum

Herausgeber:



scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:



Marc Ruff
Security Consultant
T +41 44 404 13 13
<mailto:maru@scip.ch>

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich Information Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, Trend-Micro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)