

## Contents

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

### 1. Editorial

#### Unterschätze nie den Makrovirus

Alle, die sich schon länger für Computersicherheit interessieren, können sich noch an die populären Makroviren Melissa und ILOVEYOU erinnern. Anfang des neuen Jahrtausends haben diese bis dahin unbekannt grosses Aufsehen in den Tagesmedien erregt. Office-Dokumente wurden mit korruptem Programmcode versehen, der sich selber per Email weitergeschickt hat. Die neue Gefahr schien bedrohlicher zu sein als alles, was bisher da gewesen war (was in erster Linie mit der jungen Popularität des Internets zu tun hatte).

Seitdem ist es eigentlich ruhig geworden um Makroviren. Die Antiviren-Hersteller versuchen schön artig die bekannten Abkömmlinge zu entdecken. Und selbst Microsoft hat dazugelernt, indem es in den jüngeren Versionen der Office-Suite standardmässig die Ausführung von Makros gar nicht mehr. Entweder muss der Benutzer diese Option in mühsamer und manueller Weise über die überladenen Konfigurationseinstellungen aktivieren. Oder durch eine grössflächige Warnmeldung wird er beim Öffnen eines potentiellen Makrodokuments auf die drohenden Gefahren hingewiesen (oder spätestens beim MAPI-Zugriff auf Outlook).

Wieso sollte man sich also noch mit Makroviren auseinandersetzen? Ganz einfach: Weil sie viel zu sehr unterschätzt sind! Makros sind eingebettete Skripte in Office-Dokumenten. Diese Skripte werden in einem speziellen Bereich der Datei untergebracht und können bei der reinen Interpretation des Dokuments, zum Beispiel in Word, nicht ohne weiteres gesehen werden.

Als Skriptsprache wird hierbei Visual Basic for Applications, das mit VBA abgekürzt wird, eingesetzt. Bei VBA handelt es sich um eine bisweilen vereinfachte (und manchmal arg vermurkste) Variante des klassischen Visual Basic 6.0 (VB6). Die Möglichkeiten sind weitestgehend die Gleichen. Auf der Codeebene kann zu 99% die identische Funktionalität erreicht werden. Nur in Bezug auf das Design der grafischen Oberfläche hat sich Microsoft nicht die gleiche Mühe gegeben. Da korrupter Programmcode aber nur in den wenigstens Fällen auf schöne GUI-Elemente und OCX-Funktionen angewiesen ist, kann dies getrost vernachlässigt werden.

Die unterschiedlichen Office-Dokumente erlauben es, mittels VBA-Makros gewisse Abläufe komplexerer Natur automatisieren zu können. Zum Beispiel kann in Excel beim Verändern eines Zelleninhalts ebenfalls die Schriftart der gesamten Spalte angepasst werden. Dies wäre ohne VBA nur mit manuellen Anpassungen (oder einer Bedingten Formatierung) umsetzbar gewesen. Gerade bei grösseren und wiederkehrenden Aufgaben, die sich nicht durch simple Excel-Formeln automatisieren lassen, wird VBA zu einem nützlichen Werkzeug.

Die Entwickler korrupten Programmcodes interessieren sich aber viel mehr für andere Funktionalitäten. Zum Beispiel die Möglichkeit lesend oder schreiben auf das Dateisystem zuzugreifen. Oder weitere Dateien bzw. Programme zu öffnen. Oder gar im Netzwerk Daten zu übertragen. Wer im Umgang mit VB6 ein bisschen geübt ist, der wird derlei Routinen sehr schnell ebenfalls in VBA adaptieren können. Portierungen sind zu 95% mit simplem Copy&Paste umzusetzen. Einige Kleinigkeiten müssen dann noch den sprachspezifischen



Eigenarten angepasst werden. Ein Word-Dokument, das eine spezifische Datei aus einem Netzwerk herauschickt, bastle ich in wenigen Minuten zusammen - Und sie wird nicht von einer Antiviren-Lösung entdeckt werden!

In vielen Unternehmen sind Makros (wieder) geduldet. Man verlässt sich hierbei rigoros auf die Sicherheit der installierten Antiviren-Produkte. Diese sollen die bösartigen Makros frühzeitig erkennen und reagieren können. Doch nach wie vor werden dabei in erster Linie reaktionäre Mechanismen eingesetzt, die neuartige Viren und Würmer nicht erkennen können. Ich entwickle regelmässig neuen korrupten Programmcode für Kunden, die einen Proof-of-Concept für unsere Voraussagen sehen wollen. Man ist sodann vom Resultat hin- und hergerissen: Einerseits ist man verblüfft über die Möglichkeiten, die man da ausschöpfen kann - Andererseits ist es beängstigend zu sehen, dass auch nach 10 Jahren scheinbar plumpe und belächelte Angriffstechniken wie VBA-Makroviren zum Ziel führen können. Da nützen auch teure Firewalls, strenge Authentisierung und ein VPN-Tunnel nichts.

Die einzige Lösung besteht darin, aktive Inhalte in Dokumenten zu verbieten. In Office-Dokumenten haben VBA-Objekte nichts verloren. Und im Übrigen hat Actionscript - eine abgespeckte Version von Javascript - in PDF-Dateien ebenso nichts zu suchen (da kann man ebenfalls sehr schöne Effekte erzielen). Doch die Industrie bewegt sich immer weiter dahin, dass aktive Inhalte in ehemals statische Formate eingebunden werden können sollen. Erstaunt es da, dass in den neuesten ID-Tags von MP3-Dateien ebenfalls Bilder eingebettet werden können? Der nächste Pufferüberlauf-Exploit in einer Grafikengine ist sicher schon irgendwo in der Mache.

Marc Ruef <maru-at-scip.ch>  
Security Consultant  
Zürich, 25. Mai 2009

## 2. scip AG Informationen

### 2.1 Neue Webseite

Am 2. Juni 2009 wurde unsere aktualisierte Webseite live geschaltet.



Wir sind unserem bewährten und geschätzten CD/CI treu geblieben. Der Inhalt wurde jedoch umfassend aufgewertet.

Eines der verfolgten Ziele bei der Überarbeitung unserer Webseite war die Schaffung einer grösseren Transparenz im Bezug zu unserem täglichen Schaffen. Dies im Einklang mit den Anforderungen unserer Kunden in Bezug auf Diskretion.

Zusammengefasst bietet die neue Webpräsenz Ihnen als Besucher ein Mehr an Informationen:

- [Labs](#)
- [News](#)
- [Publikationen](#)
- [Methoden](#)
- [Referenzen](#)
- [Dienstleistungen](#)

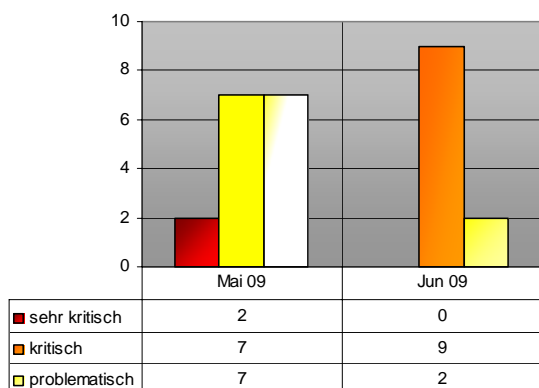
Statten Sie uns doch virtuell einen Besuch ab unter <http://www.scip.ch>. Wir freuen uns über Ihre Anregungen. Zögern Sie nicht uns diese mitzuteilen.

### 3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.



Die Dienstleistungspakete [\)scip\( pallas](#) liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.



#### Contents:

- 3990 Microsoft Windows Print Spooler Laden beliebiger DLLs
- 3989 Microsoft Windows Print Spooler Separator Pages Pufferüberlauf
- 3988 Microsoft Windows Print Spooler EnumeratePrintShares() Pufferüberlauf
- 3987 Microsoft Internet Explorer Row Reference Call Memory Corruption
- 3986 Microsoft Internet Explorer getElementByTagName() Pufferüberlauf
- 3985 Microsoft Internet Explorer EventHandler Pufferüberlauf
- 3984 Microsoft Internet Explorer setCapture() Pufferüberlauf
- 3983 Microsoft Internet Explorer xmlhttpRequest Pufferüberlauf
- 3982 Microsoft Internet Explorer DHTML Call Pufferüberlauf
- 3981 Microsoft Internet Explorer Cache Information Disclosure
- 3980 Apple iTunes Protocol Handler Pufferüberlauf
- 3979 Microsoft DirectShow QuickTime Parsing Code Execution

#### 3.1 Microsoft Windows Print Spooler Laden beliebiger DLLs

Einstufung: **problematisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3990>

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. In einem Advisory berichtet Microsoft von einer Schwachstelle im MS Print Spooler, bei der der Printspooler via eines bestimmten RPC dazu gebracht werden kann beliebige DLLs zu laden und beliebigen Code auszuführen.

#### Expertenmeinung:

Drei Schwachstellen im Print Spooler diverser Windows Versionen sind sicherlich für viele Administratoren eine eher unangenehme Angelegenheit. Zumal die Schwachstellen als kritisch anzusehen sind, gilt es hier rasch Gegenmassnahmen zu ergreifen und die entsprechenden Patches zum Einsatz zu bringen.

#### 3.2 Microsoft Windows Print Spooler Separator Pages Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3989>

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. In einem Advisory berichtet Jun Mao (via iDefense) von einer Schwachstelle im MS Print Spooler, bei der beim Parsing von Separator Pages eine Memory Corruption verursacht werden kann, die zu einem Pufferüberlauf führt.

#### Expertenmeinung:

Drei Schwachstellen im Print Spooler diverser Windows Versionen sind sicherlich für viele Administratoren eine eher unangenehme Angelegenheit. Zumal die Schwachstellen als kritisch anzusehen sind, gilt es hier rasch Gegenmassnahmen zu ergreifen und die entsprechenden Patches zum Einsatz zu bringen.

### 3.3 Microsoft Windows Print Spooler EnumeratePrintShares() Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3988>

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. In einem Advisory berichtet Jun Mao (via iDefense) von einer Schwachstelle im MS Print Spooler, bei der durch einen Fehler in EnumeratePrintShares() ein Pufferüberlauf provoziert und beliebiger Code zur Ausführung gebracht werden kann.

#### Expertenmeinung:

Drei Schwachstellen im Print Spooler diverser Windows Versionen sind sicherlich für viele Administratoren eine eher unangenehme Angelegenheit. Zumal die Schwachstellen als kritisch anzusehen sind, gilt es hier rasch Gegenmassnahmen zu ergreifen und die entsprechenden Patches zum Einsatz zu bringen.

### 3.4 Microsoft Internet Explorer Row Reference Call Memory Corruption

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3987>

Windows Internet Explorer (früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei

älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. Nils (via ZDI) beschreibt in einem Advisory die Möglichkeit, mittels speziell präparierten HTML Row Property Referenzen einen Pufferüberlauf zu verursachen und beliebigen Code zur Ausführung zu bringen.

#### Expertenmeinung:

Acht kritische Schwachstellen gibt es diesen Monat in Microsofts Standardbrowser zu beklagen. Alle dieser Schwachstellen erlauben bei richtigem Exploiting die Ausführung beliebigen Codes im Kontext der Applikation, was als grundsätzlich kritisch zu werten ist. Es empfiehlt sich daher, zeitnah um das Einspielen des zur Verfügung gestellten Patches seitens Microsoft bemüht zu sein.

### 3.5 Microsoft Internet Explorer getElementByTagName() Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3986>

Windows Internet Explorer (früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. Gemäss eines Advisories von team509 ist es mittels wiederholter Calls zu "getElementByTagName()" möglich, mittels eines Pufferüberlauf eines Eventhandlers beliebigen Code zur Ausführung zu bringen.

#### Expertenmeinung:

Acht kritische Schwachstellen gibt es diesen Monat in Microsofts Standardbrowser zu beklagen. Alle dieser Schwachstellen erlauben bei richtigem Exploiting die Ausführung beliebigen Codes im Kontext der Applikation, was als grundsätzlich kritisch zu werten ist. Es empfiehlt sich daher, zeitnah um das Einspielen des zur Verfügung gestellten Patches seitens Microsoft bemüht zu sein.

### 3.6 Microsoft Internet Explorer EventHandler Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja

Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3985>

Windows Internet Explorer (früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. team509 fand eine Schwachstelle, die bei wiederholten Calls zu Eventhandlern auftritt, wenn vorgängig Nodes zu einem HTML Dokument hinzugefügt wurden. Dies kann ebenfalls zu einer Memory Corruption führen, die die Ausführung beliebigen Codes ermöglicht.

#### Expertenmeinung:

Acht kritische Schwachstellen gibt es diesen Monat in Microsofts Standardbrowser zu beklagen. Alle dieser Schwachstellen erlauben bei richtigem Exploiting die Ausführung beliebigen Codes im Kontext der Applikation, was als grundsätzlich kritisch zu werten ist. Es empfiehlt sich daher, zeitnah um das Einspielen des zur Verfügung gestellten Patches seitens Microsoft bemüht zu sein.

### 3.7 Microsoft Internet Explorer setCapture() Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3984>

Windows Internet Explorer (früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. Peter Vreugdenhill fand eine Schwachstelle, bei der der Aufruf von setCapture() dazu genutzt werden kann, eine Memory Corruption zu provozieren und beliebigen Code zur Ausführung zu bringen.

#### Expertenmeinung:

Acht kritische Schwachstellen gibt es diesen Monat in Microsofts Standardbrowser zu beklagen. Alle dieser Schwachstellen erlauben bei richtigem Exploiting die Ausführung beliebigen Codes im Kontext der Applikation,

was als grundsätzlich kritisch zu werten ist. Es empfiehlt sich daher, zeitnah um das Einspielen des zur Verfügung gestellten Patches seitens Microsoft bemüht zu sein.

### 3.8 Microsoft Internet Explorer xmlHttpRequest Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3983>

Windows Internet Explorer (früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. Ein anonymer Researcher via ZDI fand eine Schwachstelle, bei der eine grosse Anzahl von asynchronen XMLHttpRequests genutzt werden kann, um eine Memory Corruption herbeizuführen und beliebigen Code zur Ausführung zu bringen.

#### Expertenmeinung:

Acht kritische Schwachstellen gibt es diesen Monat in Microsofts Standardbrowser zu beklagen. Alle dieser Schwachstellen erlauben bei richtigem Exploiting die Ausführung beliebigen Codes im Kontext der Applikation, was als grundsätzlich kritisch zu werten ist. Es empfiehlt sich daher, zeitnah um das Einspielen des zur Verfügung gestellten Patches seitens Microsoft bemüht zu sein.

### 3.9 Microsoft Internet Explorer DHTML Call Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3982>

Windows Internet Explorer (früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. Haifei fand eine Schwachstelle bei Calls zu DHTML Objekten, die dazu genutzt werden kann eine Memory

Corruption herbeizuführen und beliebigen Code zur Ausführung zu bringen.

#### Expertenmeinung:

Acht kritische Schwachstellen gibt es diesen Monat in Microsofts Standardbrowser zu beklagen. Alle dieser Schwachstellen erlauben bei richtigem Exploiting die Ausführung beliebigen Codes im Kontext der Applikation, was als grundsätzlich kritisch zu werten ist. Es empfiehlt sich daher, zeitnah um das Einspielen des zur Verfügung gestellten Patches seitens Microsoft bemüht zu sein.

### 3.10 Microsoft Internet Explorer Cache Information Disclosure

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 09.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3981>

Windows Internet Explorer (früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95 A ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Windows Internet Explorer 8. Jorge Luis Alvarez Medina fand in diversen Versionen eine Schwachstelle, bei der durch einen Fehler bei der Verarbeitung von gecachetem Content sensitive Daten ausgelesen werden können.

#### Expertenmeinung:

Acht kritische Schwachstellen gibt es diesen Monat in Microsofts Standardbrowser zu beklagen. Alle dieser Schwachstellen erlauben bei richtigem Exploiting die Ausführung beliebigen Codes im Kontext der Applikation, was als grundsätzlich kritisch zu werten ist. Es empfiehlt sich daher, zeitnah um das Einspielen des zur Verfügung gestellten Patches seitens Microsoft bemüht zu sein.

### 3.11 Apple iTunes Protocol Handler Pufferüberlauf

Einstufung: **problematisch**  
 Remote: Ja  
 Datum: 02.06.2009  
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3980>

iTunes ist ein Multimedia-Verwaltungsprogramm von Apple zum Abspielen, Konvertieren, Organisieren und Kaufen von Musik, Filmen und

Spielen. Es kann die Inhalte angeschlossener iPods und iPhones verwalten. iTunes wird aktuell für die Plattformen Mac OS X, Windows XP und Windows Vista weiterentwickelt. Für Mac OS 9 und Windows 2000 sind ältere Versionen erhältlich, die aber z. B. das iPhone 3G nicht mehr unterstützen. Rob King entdeckte eine Schwachstelle in verschiedenen URL Handlern, die zur Auslösung eines Pufferüberlaufs genutzt werden kann.

#### Expertenmeinung:

Die genannte Schwachstelle ist als problematisch einzustufen. Betroffene Installationen sollten zeitnah auf den neusten Stand (8.2) gebracht werden, um eine Kompromittierung zu vermeiden.

### 3.12 Microsoft DirectShow QuickTime Parsing Code Execution

Einstufung: **sehr kritisch**  
 Remote: Ja  
 Datum: 29.05.2009  
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3979>

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. In einem jüngst, ausserplanmässig erschienen Advisory beschreibt Microsoft eine Lücke, die derzeit aktiv als 0-Day ausgenutzt wird. Durch einen nicht näher spezifizierten Fehler in quartz.dll, kann ein Angreifer über Quicktime Media Files beliebigen Code zur Ausführung bringen.

#### Expertenmeinung:

Die vorliegende Lücke ist ohne jeden Zweifel kritisch und sollte mit höchster Aufmerksamkeit verfolgt werden. Durch die Tatsache, dass diese Lücke bereits aktiv ausgenutzt wird, erhöht sich die Gefahr einer potenziellen oder bereits erfolgten Kompromittierung. Administratoren sollten daher die Empfehlungen des Herstellers ausführlich lesen und sich über die Entwicklung in dieser Sache auf dem Laufenden halten.

## 4. Statistiken Verletzbarkeiten

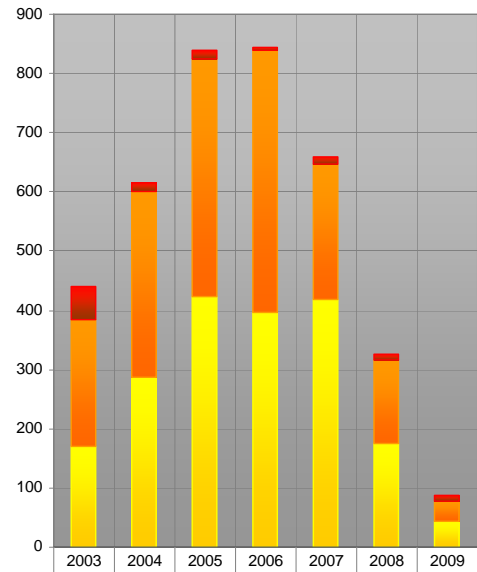
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

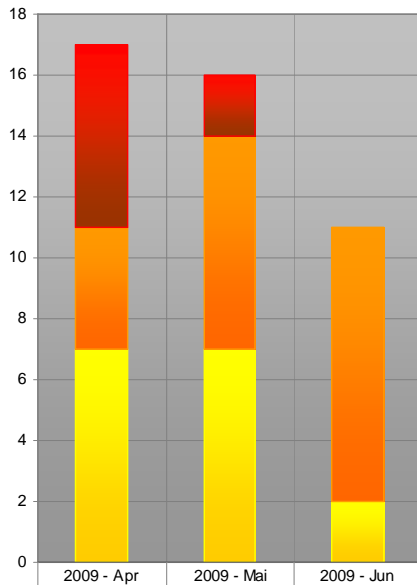
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum: 19. Mai 2009



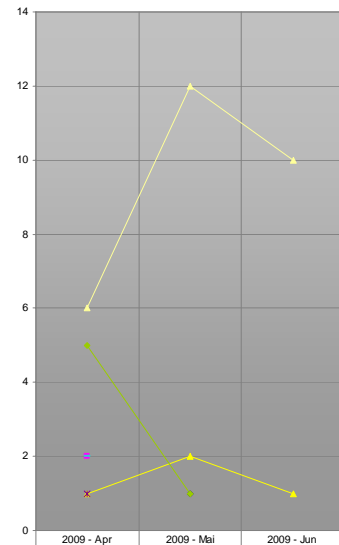
	2003	2004	2005	2006	2007	2008	2009
sehr kritisch	56	15	15	6	11	11	9
kritisch	214	314	402	442	229	140	34
problematisch	170	287	423	396	419	176	44

Verlauf der Anzahl Schwachstellen pro Jahr



	2009 - Apr	2009 - Mai	2009 - Jun
sehr kritisch	6	2	
kritisch	4	7	9
problematisch	7	7	2

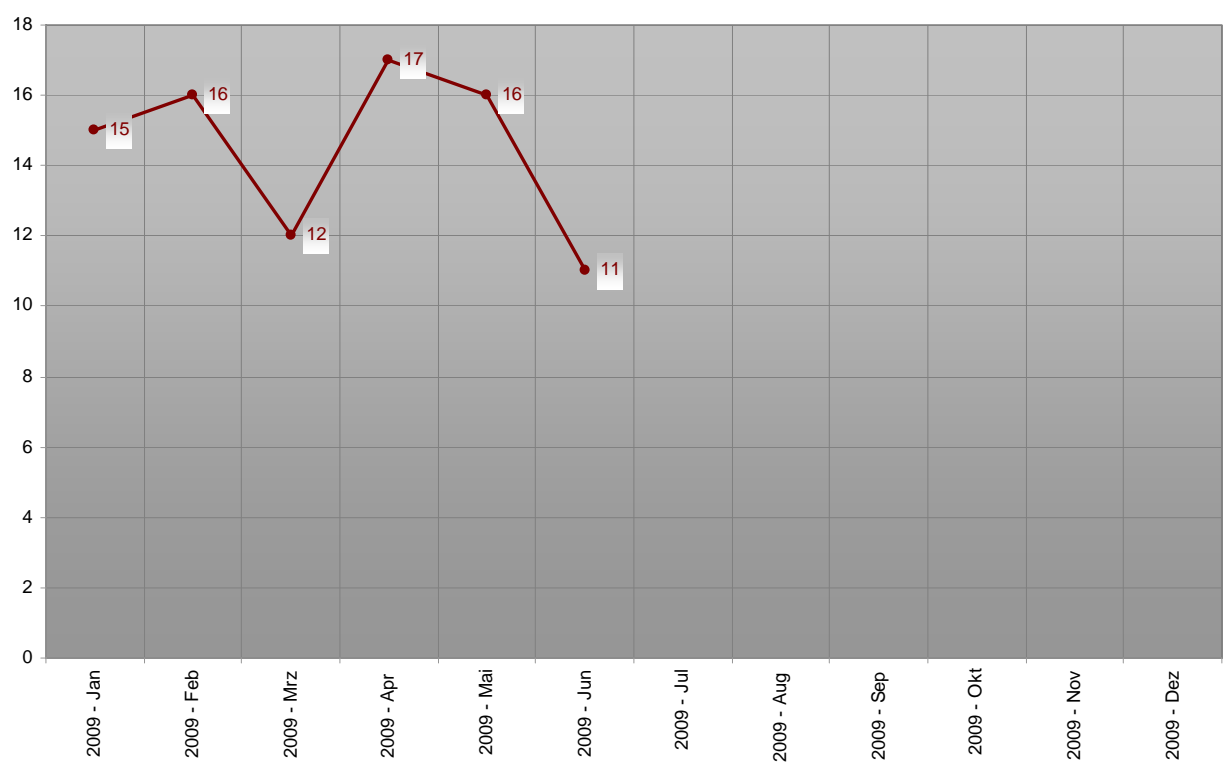
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



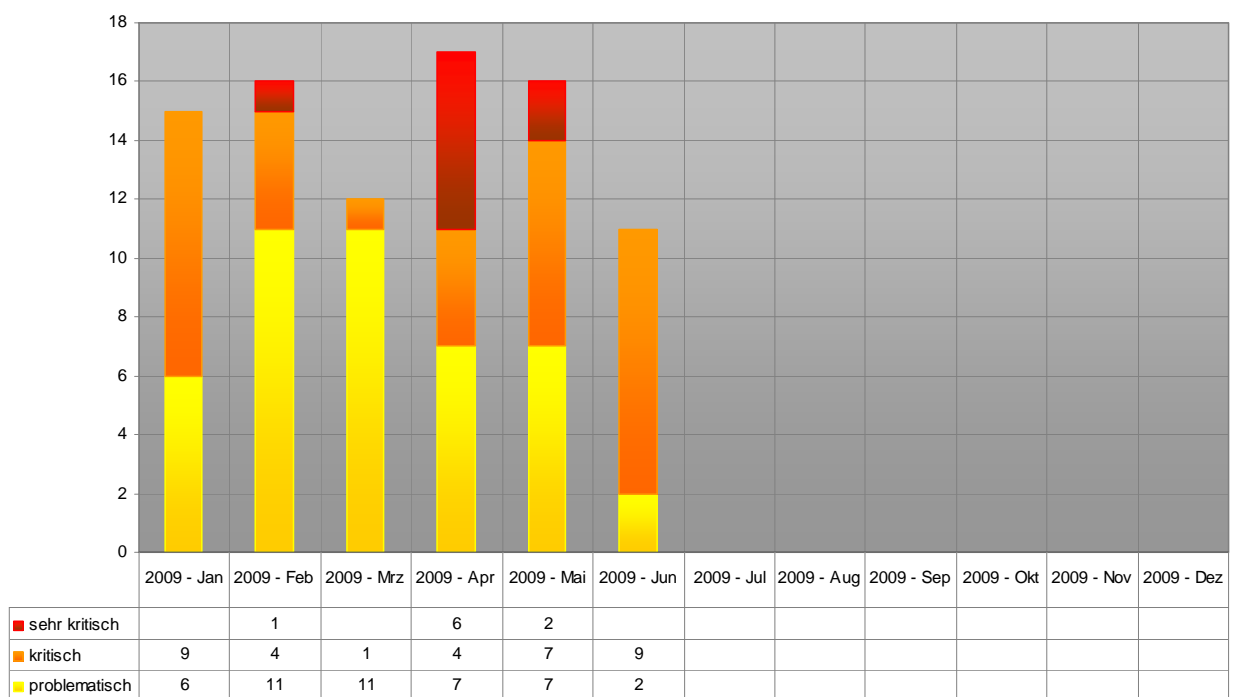
	2009 - Apr	2009 - Mai	2009 - Jun
Cross Site Scripting (XSS)		1	
Denial of Service (DoS)	2		
Designfehler	1	2	1
Directory Traversal			
Eingabeungültigkeit	1		
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Format String			
Konfigurationsfehler			
Pufferüberlauf	6	12	10
Race-Condition			
Schwache Authentifizierung			
Schwache			

Verlauf der letzten drei Monate Schwachstelle/Kategorie

Registrierte Schwachstellen by scip AG



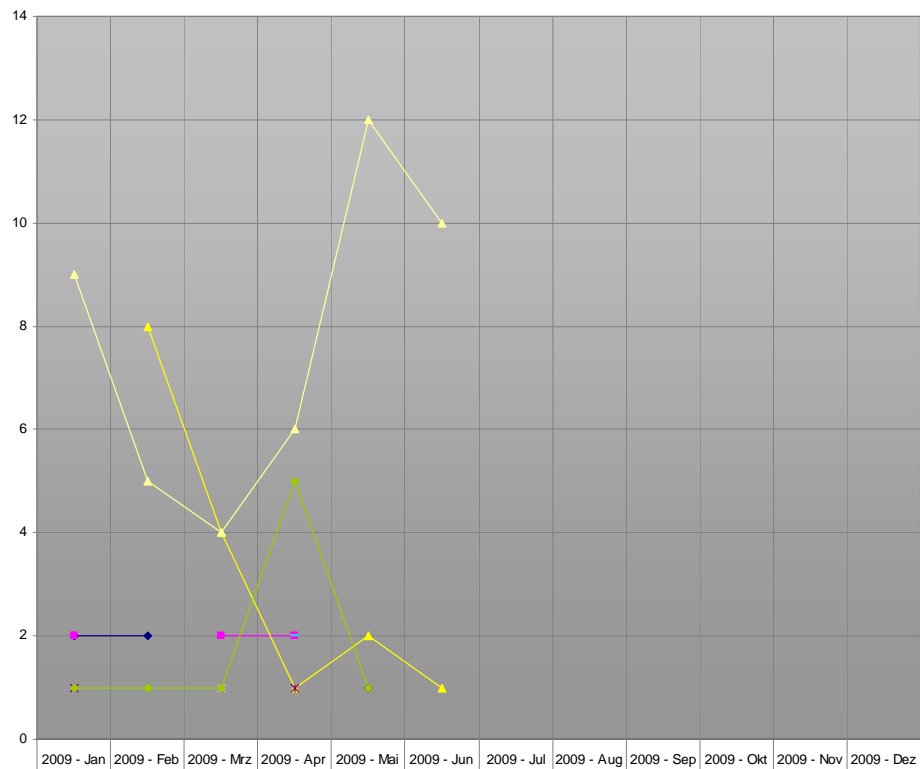
Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008-2009



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2009

scip monthly Security Summary 19.06.2009

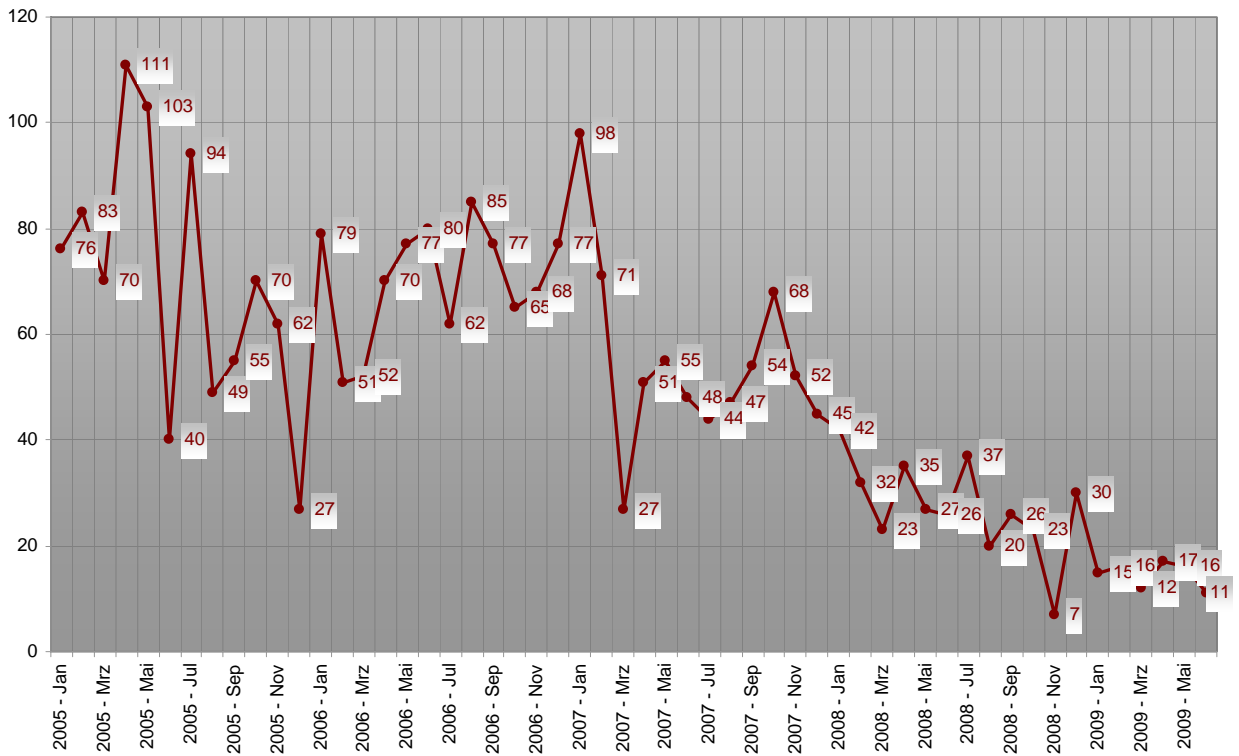




	2009 - Jan	2009 - Feb	2009 - Mrz	2009 - Apr	2009 - Mai	2009 - Jun	2009 - Jul	2009 - Aug	2009 - Sep	2009 - Okt	2009 - Nov	2009 - Dez
◆ Cross Site Scripting (XSS)	2	2			1							
■ Denial of Service (DoS)	2		2	2								
▲ Designfehler		8	4	1	2	1						
✕ Directory Traversal												
✖ Eingabeungültigkeit	1			1								
● Fehlende Authentifizierung												
✚ Fehlende Verschlüsselung												
— Fehlerhafte Leserechte												
— Fehlerhafte Schreibrechte												
— Format String												
— Konfigurationsfehler												
▲ Pufferüberlauf	9	5	4	6	12	10						
✕ Race-Condition												
✖ Schwache Authentifizierung			1									
✖ Schwache Verschlüsselung												
— SQL-Injection												
— Symink-Schwachstelle												
— Umgehungs-Angriff				2								
◆ Unbekannt	1	1	1	5	1							

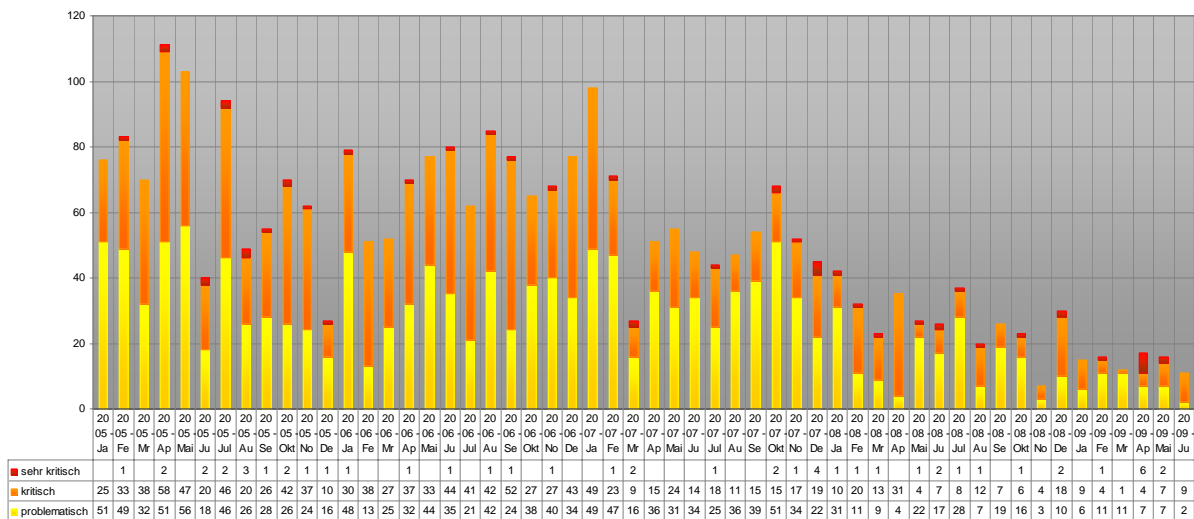
Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2009

Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005

scip monthly Security Summary 19.06.2009



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005





## 5. Bilderrätsel



GESUCHTE BEGRIFFE		
4 (english)	4 (english)	4 (Deutsch)

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 **15.06.2009**. 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> unter Publikationen > scip monthly Security Summary > Errata.

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

### SECURITYTRACKER



## 6. 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 IT-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, TrendMicro, 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](mailto:smss-feedback@scip.ch). Das **Errata** (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summaries finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)