

Contents

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

1. Editorial

Ein Geschäft für Antiviren-Hersteller

Ich habe mich sehr früh angefangen für Computerviren zu interessieren. Im Alter von etwa 13 Jahren hatte ich schon eine ganze Reihe von Viren für meinen MS DOS 3.1 Rechner geschrieben. Dabei haben mich weniger die Schadroutinen, sondern viel mehr die Möglichkeiten effizienter Infektionen sowie das Verstecken von Antiviren-Mechanismen interessiert. Da ich zeitgleich eine eigene Antiviren-Routine (in erster Linie auf der Basis einer Mustererkennung) schrieb, empfand ich das Entwickeln meiner Viren und das Erweitern meiner Antiviren-Software als virtuelles Schachspiel gegen mich selber.

Das Interesse an korruptem Programmcode habe ich, auch wenn ich mich zwischenzeitlich eher anderen Gebieten wie der Netzwerksicherheit zugewandt habe, nie wirklich verloren. Der Fortschritt in der Antiviren-Industrie ist dabei genauso interessant zu beobachten wie die immer komplexer (und leider qualitativ oft schlechter) gewordenen Computerviren (die Motive der Virenentwickler haben sich zunehmend den kapitalistischen Zeiten

angepasst und damit die enthusiastische Tragweite ihrer Arbeiten).

Das Wissen aus diesen Bereichen war und bleibt bis zu einem hohen Grad sehr exklusiv. Vor 15 Jahren konnte man die Grundlagen in wenigen trockenen Büchern, die irgendwo in der hiesigen Bibliothek neben C64-Büchern verstaubten, nachlesen (sehr zu empfehlen ist *The Giant Black Book of Computer Viruses*). Heute kann man zwar auf ein Mehr an sehr guten Fachpublikationen zurückgreifen (zu empfehlen ist *The Art of Computer Virus Research and Defense*). Die Komplexität moderner Computersysteme führte jedoch dazu, dass der Aufwand für das Erarbeiten des grundlegenden Verständnisses um ein Vielfaches zugenommen hat.

Die Entwickler von Antiviren-Lösungen wissen, dass ihre Kunden zu einem überwiegenden Teil wenig Ahnung von der Funktionsweise ihrer Software und den Möglichkeiten moderner Computerviren haben. Wieviele Benutzer wissen schon, dass das grundlegende Prinzip der vermeintlich hochkomplexen Produkte lediglich darauf basiert, dass Dateien nach für korrupten Programmcode bekannte Zeichenketten (Pattern-Matching) durchsucht werden? Ergo kann eine Antiviren-Lösung nur Schädlinge erkennen, die durch den Hersteller zuvor entdeckt, analysiert und dokumentiert wurden. Neue Entwicklungen, die dieses Prinzip technisch und wirtschaftlich abzulösen in der Lage sind, sind bis auf weiteres nicht erkennbar (Heuristische Methoden sind zu grossen Teilen noch immer nicht ausgefeilt).



Der spanische Antiviren-Hersteller Panda hat vor einiger Zeit den freien Online-Scanner ActiveScan 2.0 vorgestellt. Durch ein Browser-Plugin, das ebenfalls mit Mozilla Firefox funktioniert und nur die Installation einer dubiosen EXE-Datei erfordert, kann der Besucher sein System auf bekannten Schadcode hin untersuchen lassen. In einer kleinen Übersicht werden dann die Infektionen gezeigt. Einige von ihnen lassen sich mit der Gratisversion beheben, andere erfordern den

Kauf der Vollversion. Auf der Eingangsseite wird der Besucher mit dem Hinweis "23% of PCs with antivirus are infected" empfangen (Stand 22. August 2008). Die Antiviren-Industrie ist also unser aller Retter oder wenigstens 23% der Computerbenutzer, die ja schon eine Antiviren-Lösung einsetzen. Wie hoch wird denn die Infektionsrate bei Systemen erwartet, die noch kein solches (Konkurrenz-)Produkt einsetzen?

Wirkliche Details liefert die grafischer Oberfläche des Online-Scanners nicht. Dass da aber ebenfalls unkritische Elemente (z.B. Tracking-Cookies) als böartigen und nur mit der Vollversion entfernbare Objekte ausgewiesen werden, grenzt schon an Bauernfängerei. Um diese Cookies zu entfernen, reicht schliesslich das Anpassen der Konfiguration des Webbrowsers oder halt die Nutzung einer freien Lösung wie Spybot-S&D.

Die Antiviren-Hersteller kämpfen um ihre Kunden. Und sie tun dies ganz offensichtlich mit zwielichtigen Mitteln, wie selbst Eva Chen von TrendMicro im Interview mit ZDNet UK zugibt ("In the antivirus business, we have been lying to customers for 20 years."). Da werden Mitbewerber mit giftigen Werbesprüchen angegriffen (23% aller mit einer Antiviren-Lösung bestückten Systeme sind infiziert), Gefahren heraufgespielt (Cookies als Schadcode) und möglichst viele Anwendungen als potentiell schädlich ausgewiesen (Security-Tools als Schadcode), um das eigene Produkt als absolute Lösung anpreisen zu können. Der Benutzer wird mit statistisch unhaltbaren Prozentangaben (23%) und rot blinkenden Warnhinweisen vorgegakuelt, dass alle Leute im Internet was Böses im Schilde führen. Schnell, schnell, wir müssen die neueste Version von Panda Antivirus kaufen - Ist die Advanced Extended 2009 Ultimate Professional Edition denn noch nicht draussen!?

Die Antiviren-Industrie darf man, abgesehen vom Bereich der Kryptografie, als klassische Disziplin der Computersicherheit schlechthin bezeichnen. Lange bevor es Firewalls und Vulnerability Scanner gab, wurden schon Viren wie der Brain- oder Cascade-Virus erfolgreich gesucht. Dennoch dümpelt die Branche auch nach 20 Jahren noch mit unsauberen Mechanismen und stümperhaften Methoden vor sich hin. Ohne eine Verbesserung in fünf wichtigen Bereichen werden Antiviren-Lösungen auch weiterhin ihre echte Nützlichkeit nicht entfalten können:

1) Werbe-Ethik: Hersteller von Antiviren-Lösungen müssen ihre Kunden sehr genau auf die Funktionsweise und Möglichkeiten

(was kann man und was kann man eben nicht) ihrer Produkte hinweisen. Draufgängerische Parolen wie "100%iger Schutz" gehören verboten.

- 2) Einheitliche Identifikation: Es fehlt nach wie vor ein einheitliches System zur Identifikation von Schadcode durch verschiedene Produkte, ähnlich der CVE-Identifikation bei Sicherheitslücken. (Einige Produkte finden HackTool.Win32.AttKit.c wobei es andere als W32/VirTool.ES bezeichnen.)
- 3) Einheitliche Terminologie: Man konnte sich in einigen Punkten noch immer nicht auf eine einheitliche und nachvollziehbare Terminologie für Schadcode und dessen Eigenschaften einigen. Der Fund von Exploits und Joke-Software muss klar als solche ausgewiesen und die (oftmals unkritischen) Hintergründe erklärt werden (z.B. keine Gefahr für den Nutzer).
- 4) Klare Abgrenzung: Antiviren-Lösungen sollten klar erkennbar eine bestimmte oder bestimmbar Klasse von Schadcode determinieren können. Das Finden von Exploits und Joke-Software sollte sich explizit deaktivieren lassen. Penetration Tester wollen ebenfalls Antiviren-Produkt einsetzen, ohne ständig Meldungen zu httprecon, ATK und MetaSploit wegstutzen zu müssen.
- 5) Detaillierte Informationen: Antiviren-Produkte weisen oftmals nur oberflächliche Informationen zu vermeintlichen Findings aus. Anstelle des hauseigenen kryptischen Namens (z.B. Generic.XPL.IIS.B1F5A3B2, siehe Punkt 2 und 3) sollten technische Details zum Schadcode (z.B. welche Bereiche betroffen) sowie zur erfolgreichen Erkennung (z.B. welche Muster sind vorhanden) ausgewiesen werden. Eine umfassende öffentliche Datenbank ist wünschenswert.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 23. Februar 2009

2. scip AG Informationen

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

2.1 Web Application Penetration Test

Die Welt ohne Internet und ohne Webseiten ist nicht mehr vorstellbar. Keine Firma ohne Webauftritt! Die Ausprägung beginnt bei einfachen „Visitenkarten im Netz“ über interaktive Firmenvorstellungen mit notwendiger Softwareinstallation im Client-Browser bis hin zu komplexen Webapplikationen mit Datenbankbindung wie E-Banking oder Online-Shops. Alle Personen mit Zugang zum Internet haben somit Zugriff auf die so bereitgestellten Daten.

Die Herausforderung beginnt nun damit, dass übliche Sicherheitsmassnahmen wie Firewalls oder Antiviren Lösungen nicht den notwendigen Schutz bieten können. Erschwerend kommt dazu, dass Software von Menschen programmiert wird und selten ohne Fehl und Tadel ist.

Die Grosse Frage lautet nun: wie kann ich meinen Kunden, Interessenten und Partner Zugriff auf meine Webseite und Dienste gewähren ohne, dass ich oder meine Dienstleister und Webseitenbenutzer befürchten müssen Opfer von zum Beispiel einfachem Vandalismus, Erpressung, Datendiebstahl oder Informationsmanipulation zu werden?

Diese Fragestellung lässt sich durch Webapplication Penetration Tests beantworten. Nach der Definierung der Risikoklassifizierung und den zu erwartenden Angreifertypen werden zielgerichtete, kundenbasierende und lösungsorientierte Testreihen umgesetzt um die Sicherheit Ihrer Webangebote zu determinieren, detaillierte Gegenmassnahmen zu planen und die definierte Sicherheit Ihrer Werte langfristig zu sichern.

Dank unserer langjährigen Erfahrung in diesem spezifischen Gebiet inklusive der Programmierung eigener Penetration Test Software und unserem ausgewiesenen Expertenwissen haben wir als scip AG die Ehre die unterschiedlichsten Webapplikationen (E-Banking, Online-Shop etc.) vieler namhafter nationaler- und internationaler Unternehmungen überprüft zu haben und dabei geholfen haben diese abzusichern.

Zählen auch Sie auf uns!

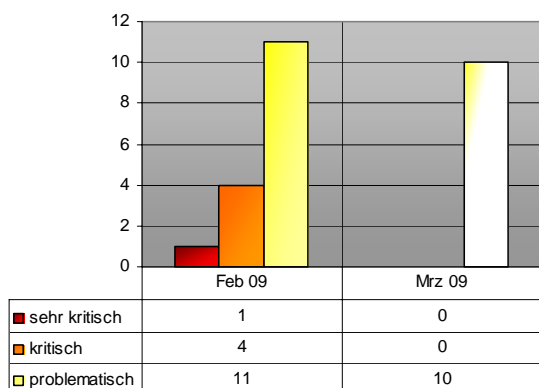
Zögern Sie nicht und kontaktieren Sie unseren

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:

- 3943 BlueCoat ProxySG SSH DoS Verletzbarkeit
- 3941 Lotus Notes 6 File Viewer Schwachstelle
- 3940 Cisco Unified Communications Manager IP Phone Verletzbarkeit
- 3939 Microsoft Windows DNS mehrere Verletzbarkeiten
- 3938 Microsoft Windows SSL Schwachstelle
- 3937 Microsoft Windows mehrere Verletzbarkeiten
- 3936 Foxit Reader mehrere Verletzbarkeiten
- 3935 Mozilla Firefox mehrere Verletzbarkeiten
- 3934 Blue Coat ProxySG HTTP "Host:" Sicherheitsumgehung möglich
- 3933 Adobe Flash mehrere Verletzbarkeiten
- 3932 Microsoft Office Excel Falsche Objekt Referenz Verletzbarkeit
- 3931 Adobe Reader / Acrobat JBIG2 Datenreihe Indexierungs Verletzbarkeit

3.1 BlueCoat ProxySG SSH DoS Verletzbarkeit

Einstufung: **problematisch**
 Remote: Ja
 Datum: 17.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3943>

BlueCoat ist eine amerikanische Firma, welche sich auf Lösungen spezialisiert hat, welche Web Verkehr verschlüsseln. Das Produkt BlueCoat ProxySG wird dazu verwendet, den Verkehr vom und zum Internet zu filtern und zu regulieren. Die bekannt gewordene Schwachstelle betrifft das SSH Protocol 1, wo ein Denial of Service mit einem manipulierten SSH Packet provoziert werden kann.

Expertenmeinung:

BlueCoat verspricht, dass diese Schwachstelle mit dem nächsten Update gefixt werden wird. Bis zu diesem Zeitpunkt empfehlen wir, SSH generell nicht mehr in der 1. Version zu verwenden, sondern nur noch SSH V2 zuzulassen.

3.2 Lotus Notes 6 File Viewer Schwachstelle

Einstufung: **problematisch**
 Remote: Ja
 Datum: 18.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3941>

Lotus Notes ist ein Produkt welches ursprünglich von Iris Associates entwickelt und später von IBM aufgekauft wurde. Es handelt sich dabei um eine Datenbanklösung, welche auch E-Mail Anbindungen integriert hat. In der nun bekannt gewordenen Schwachstelle kann über manipulierte E-Mail Anhänge Code ausgeführt werden, welche einen Buffer Overflow provozieren.

Expertenmeinung:

Da Lotus Notes im Geschäftsfeld sehr weit verbreitet ist und die Schwachstelle von Fern ausgeführt werden kann, ist die Gefahr nicht zu unterschätzen. Die Einfachste Massnahme ist, keine unbekannt Anhänge zu öffnen, welche sie per E-Mail erhalten. Ausserdem kann der File Viewer deaktiviert werden um Gefahren zu vermeiden.

3.3 Cisco Unified Communications Manager IP Phone Verletzbarkeit

Einstufung: **problematisch**
 Remote: Nein
 Datum: 12.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3940>

Cisco ist ein amerikanisches Telekommunikationsunternehmen, welches vor allem bekannt und weit vertreten ist mit seinen Router und Switch Produkten. Zu ihrem

IP Telephony angebot gehören auch eigene Telefone, welche durch den Unified Communication Manager (UCM) gesteuert werden. Die nun veröffentlichte Schwachstelle beinhaltet einen Designfehler, bei welchem die Zugangsdaten zum UCM im Klartext ausgegeben werden und entsprechend das ganze Telefonnetzwerk manipuliert werden kann.

Expertenmeinung:

Da die Ausgabe der Daten nur im lokalen Netzwerk sichtbar sind, ist die Gefahr nicht auf höchster Stufe zu werten. Allerdings sollte so ein Fehler so schnell wie möglich gepatched werden, um eventuelle Ausnützungen zu unterbinden.

3.4 Microsoft Windows DNS mehrere Verletzbarkeiten

Einstufung: **problematisch**
 Remote: Ja
 Datum: 10.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3939>

Microsoft ist einer der grössten und bekanntesten Betriebssystemanbietern. Microsoft Windows ist als Server und Desktop Packet verfügbar und in verschiedenen Versionen verbreitet. Speziell im Desktop Umfeld ist vorallem Windows XP sehr populär, allerdings ist auch die zur Zeite neueste Version, Windows Vista, sehr bekannt. DNS wird benutzt, um Internet Adressnamen (URLs) in IP Adressen umzuwandeln und umgekehrt. In den kürzlich veröffentlichten Schwachstellen können die lokal gespeicherten Anfragen so manipuliert werden, dass erneute Aufrufe auf eine Webseite auf eine fremde Seite umgeleitet werden können.

Expertenmeinung:

Durch die sehr hohe Verbreitung von Windows Betriebssystemen, ist die Gefahr für die Ausnutzung dieser Schwachstelle sehr gross. Wir empfehlen so schnell wie möglich auf die neueste Software Version zu aktualisieren.

3.5 Microsoft Windows SSL Schwachstelle

Einstufung: **problematisch**
 Remote: Ja
 Datum: 10.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3938>

Microsoft ist einer der grössten und bekanntesten Betriebssystemanbietern. Microsoft Windows ist als Server und Desktop

Packet verfügbar und in verschiedenen Versionen verbreitet. Speziell im Desktop Umfeld ist vorallem Windows XP sehr populär, allerdings ist auch die zur Zeite neueste Version, Windows Vista, sehr bekannt. SSL wird benutzt, um eine Verbindung zu einem Server zu schützen. Dies ist über das Schlüsselsymbol in der URL Bar ihres Browsers erkennbar. Über die nun gepatchte Schwachstelle konnte die SSL Verschlüsselung aufgebaut werden, ohne das die Authentifizierung komplett überprüft wurde.

Expertenmeinung:

Durch die sehr hohe Verbreitung von Windows Betriebssystemen, ist die Gefahr für die Ausnutzung dieser Schwachstelle sehr gross. Wir empfehlen so schnell wie möglich auf die neueste Software Version zu aktualisieren.

3.6 Microsoft Windows mehrere Verletzbarkeiten

Einstufung: **problematisch**
 Remote: Ja
 Datum: 10.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3937>

Microsoft ist einer der grössten und bekanntesten Betriebssystemanbietern. Microsoft Windows ist als Server und Desktop Packet verfügbar und in verschiedenen Versionen verbreitet. Speziell im Desktop Umfeld ist vorallem Windows XP sehr populär, allerdings ist auch die zur Zeite neueste Version, Windows Vista, sehr bekannt. Der neueste Patch repariert verschiedene Schwachstellen. Zum einen kann bösartiger Code lokal ausgeführt werden, wenn EMF und WMF Bilder von manipulierten Web Seiten angeschaut werden, zum andern können durch Fehler im Kern des Betriebssystems die Authentifizierungsmöglichkeiten manipuliert werden und so höhere Rechte erworben werden.

Expertenmeinung:

Da Microsoft Betriebssysteme sehr weit verbreitet sind und zudem noch alle Versionen der letzten 8 Jahre davon betroffen sind, ist es wichtig die neuesten Patches einzuspielen. Zudem können wir generell nur empfehlen, nie Anhänge von Unbekannten zu öffnen und Meldungen, welche auf ihrem Bildschirm erscheinen nie vorschnell wegzuklicken.

3.7 Foxit Reader mehrere Verletzbarkeiten

Einstufung: **problematisch**
 Remote: Ja
 Datum: 09.03.2009

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3936>

Foxit ist ein Unternehmen, welches sich auf die Implementation von PDF Technologien konzentriert hat. Foxit Reader ist ein freies PDF Leseprogramm welches sich speziell dadurch auszeichnet, dass es sehr viel kleiner als der Adobe Reader ist und zusätzliche Funktionen verfügt. Die nun veröffentlichten Schwachstellen waren schon länger im Adobe Reader bekannt und wurden neuerdings auch aktiv im Foxit Reader ausgenutzt. Sie lässt zu, dass Schadcode mit Hilfe von speziell präparierten PDFs oder erzwungenen überlangten Dokumente Namen ausgeführt werden kann.

Expertenmeinung:

Da der Foxit Reader noch nicht allen bekannt ist, ist die Gefahr nicht ganz so gross. Allerdings war die Schwachstelle schon länger durch den Adobe Reader bekannt und wurde entsprechend schon länger ausgenutzt. Wir empfehlen, den veröffentlichten Patch so schnell wie möglich einzuspielen und generell keine Dokumente zu öffnen, welche sie nicht erwarten oder den Sender nicht kennen.

3.8 Mozilla Firefox mehrere Verletzbarkeiten

Einstufung: **problematisch**
 Remote: Nein
 Datum: 05.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3935>

Mozilla Firefox ist ein freier Webbrowser des Mozilla-Projekts. Der seit Mitte 2002 entwickelte Open-Source-Webbrowser zeichnet sich besonders durch seine vielfältigen Erweiterungsmöglichkeiten aus. Firefox ist nach dem Windows Internet Explorer der zweithäufigst genutzte Webbrowser. Durch mehrere bekannt gewordene Schwachstellen können unter anderem Sicherheitseinstellungen umgangen, sensitive Informationen ausgelesen und auf das lokal System zugegriffen werden.

Expertenmeinung:

Da der Firefox Webbrowser sehr weit verbreitet ist, ist die Gefahr für diese Schwachstelle sehr gross. Da aber bereits ein Patch herausgegeben wurde empfehlen wir, auf die neueste Version (3.0.7) zu aktualisieren. Generell empfehlen wir, Firefox so einzustellen, dass er automatisch die neuesten Updates einspielt. Falls dies bei ihrem Browser nicht der Fall ist, kann dies unter Einstellungen>Erweitert>Update entsprechend konfiguriert werden. Ihre aktuelle Version wird

über Hilfe>Über Mozilla Firefox angezeigt.

3.9 Blue Coat ProxySG HTTP "Host:" Sicherheitsumgehung möglich

Einstufung: **problematisch**
 Remote: Ja
 Datum: 03.03.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3934>

Blue Coat ProxySG ist ein weit verbreitetes Produkt, um den Datenverkehr vom Intranet zum Internet zu überwachen. Zusätzlich bietet es die Möglichkeit, bestimmte Daten zu filtern und so den Internetzugang für die Mitarbeiter einzuschränken. Die nun entdeckte Lücke erlaubt es, gesperrte Seiten zu erreichen wenn das "Host:" Attribut gefälscht wird. Blue Coat hat, um dies zu verhindern, ein Workaround publiziert welches bis zum nächsten Update ausgeführt werden soll.

Expertenmeinung:

Durch die weite Verbreitung von Blue Coat Proxies ist es entsprechend an vielen Orten möglich, Sicherheitsvorkehrungen zu umgehen. Das Ausmass hält sich aber in Grenzen, da die Umsetzung nicht für jeden Mitarbeiter technisch möglich und es so "nur" möglich ist, im Internet Seiten aufzurufen welche gesperrt worden waren.

3.10 Adobe Flash mehrere Verletzbarkeiten

Einstufung: **problematisch**
 Remote: Nein
 Datum: 25.02.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3933>

Adobe Flash ist ein Produkt von Adobe Systems. Es wird dazu benutzt, multimediale Inhalte zu erstellen und anzuschauen. Der Adobe Flash Player findet heute eine weite Verbreitung da Adobe Flash Animation mit Programmieren verbindet und entsprechend vielseitig eingesetzt werden kann. Die vorgestellten Schwachstellen betreffen mehrere Systeme und sind nicht nur einfache Eingabvalidierungen welche nicht funktionieren, sondern unter anderem auch Fehler in der Verarbeitung von Referenzen und ermöglichen das Schadcode ausgeführt werden kann.

Expertenmeinung:

Die neu gefundenen Schwachstellen sind wegen ihrer hohen Verbreitung sehr gefährlich, können aber nur lokal vom Computer ausgeführt werden.

Wir empfehlen, so schnell wie möglich auf die neuesten Versionen zu aktualisieren.

3.11 Microsoft Office Excel Falsche Objekt Referenz Verletzbarkeit

Einstufung: **kritisch**
Remote: Ja
Datum: 24.02.2009
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3932>

Microsoft Excel ist ein Tabellenkalkulationsprogramm welches inzwischen nicht nur für Microsoft Betriebssysteme sondern auch für Konkurrenzsysteme erhältlich ist. Es ist weit verbreitet im privaten wie auch im geschäftlichen Umfeld um Daten übersichtlicher Darzustellen oder um mit Daten zu rechnen. Exploits zu dieser Schwachstelle nutzen einen Designfehler aus, in dem sie auf Dokumente referenzieren welche nicht existieren. Dadurch lässt sich beliebigen Code lokal ausführen. Dieser Fehler tritt beim Öffnen einer beschädigten Excel Tabelle auf.

Expertenmeinung:

Dieser Fehler ist gefährlich, da Microsoft Excel sehr weit verbreitet ist und noch kein Patch dazu zur Verfügung gestellt wurde. Microsoft empfiehlt dazu, MOICE (Microsoft Office Isolated Conversion Environment) zu verwenden um Dokumente vor dem Öffnen zu überprüfen und so eine mögliche Verletzung zu unterbinden. Alternativ könnte auch die Microsoft Office File Block policy so eingestellt werden, dass Dokumente welche mit Office 2003 oder früher erstellt wurden, automatisch geblockt werden; Allerdings wird dies nicht für jeden zufriedenstellend sein. Grundsätzlich empfehlen wir, Dokumente von unbekanntem Absendern und/oder welche nicht angekündigt wurden nicht zu öffnen.

3.12 Adobe Reader / Acrobat JBIG2 Datenreihe Indexierungs Verletzbarkeit

Einstufung: **sehr kritisch**
Remote: Ja
Datum: 20.02.2009
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3931>

Adobe Acrobat Reader ist ein Produkt einer Gruppe von Programmen, welches zum Lesen von PDF Dateien verwendet wird. Das Programmpaket ist kostenpflichtig, der Reader ist aber auch frei und kostenlos erhältlich und entsprechend weit verbreitet. In dem jetzt

bekannt gewordenen Designfehler werden JBIG2 Daten, welche zum Verkleinern von Bildern benutzt werden, falsch indexiert und weiter verwendet. Dadurch ist es möglich, von Remote über den lokalen Speicher fremden Code auszuführen.

Expertenmeinung:

Diese Schwachstelle ist zur Zeit noch als sehr gefährlich einzustufen, da der Adobe Reader sehr verbreitet ist und auch die aktuellste Version betroffen ist. Adobe arbeitet zur Zeit an einer Behebung der Lücke und will diese am 11. März 09 veröffentlichen. In der Zwischenzeit soll man vermeiden, unbekannte oder unangemeldete PDF Dokumente von Kollegen und Fremden Personen zu öffnen. Da diese Schwachstelle aktuell bereits ausgenutzt wird, ist äusserste Vorsicht geboten.

Heute wurden die Patches für dieses Problem publiziert, sie sind erhältlich über <http://www.adobe.com/support/security/bulletins/apsb09-03.html>.

4. Statistiken Verletzbarkeiten

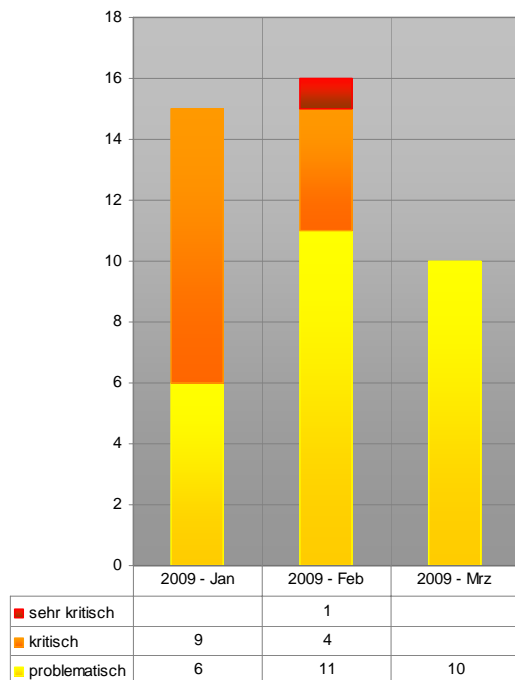
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



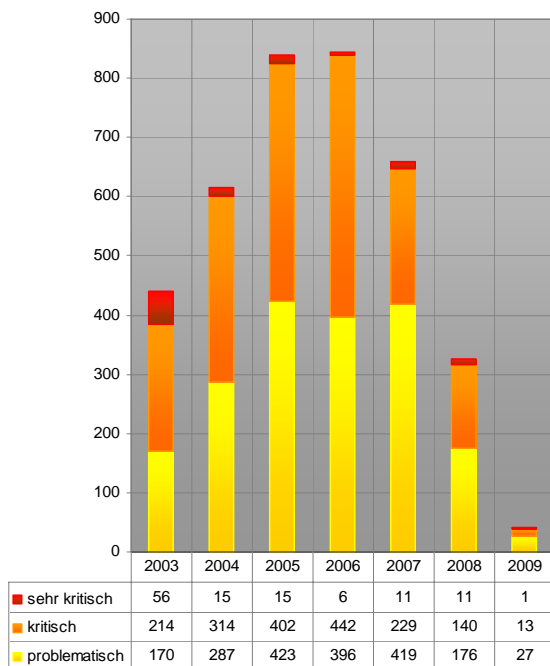
<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

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.

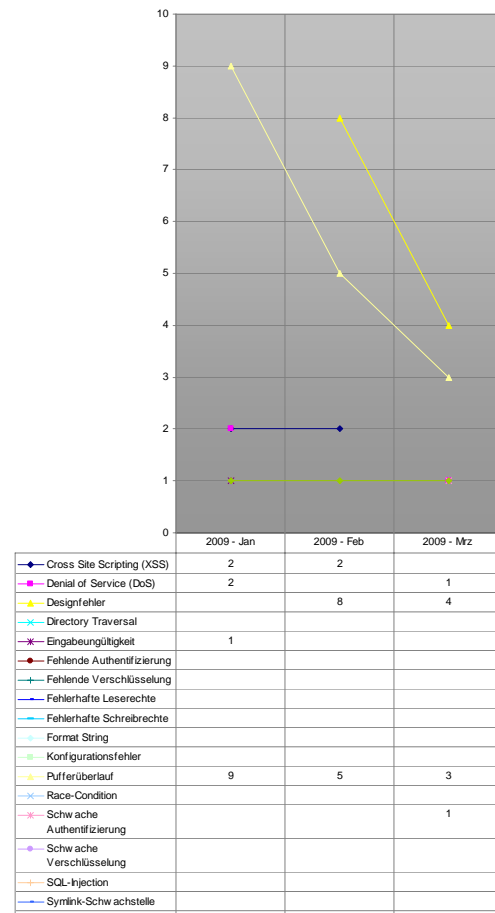
Auswertungsdatum: 19. März 2009



Verlauf der Anzahl Schwachstellen pro Jahr

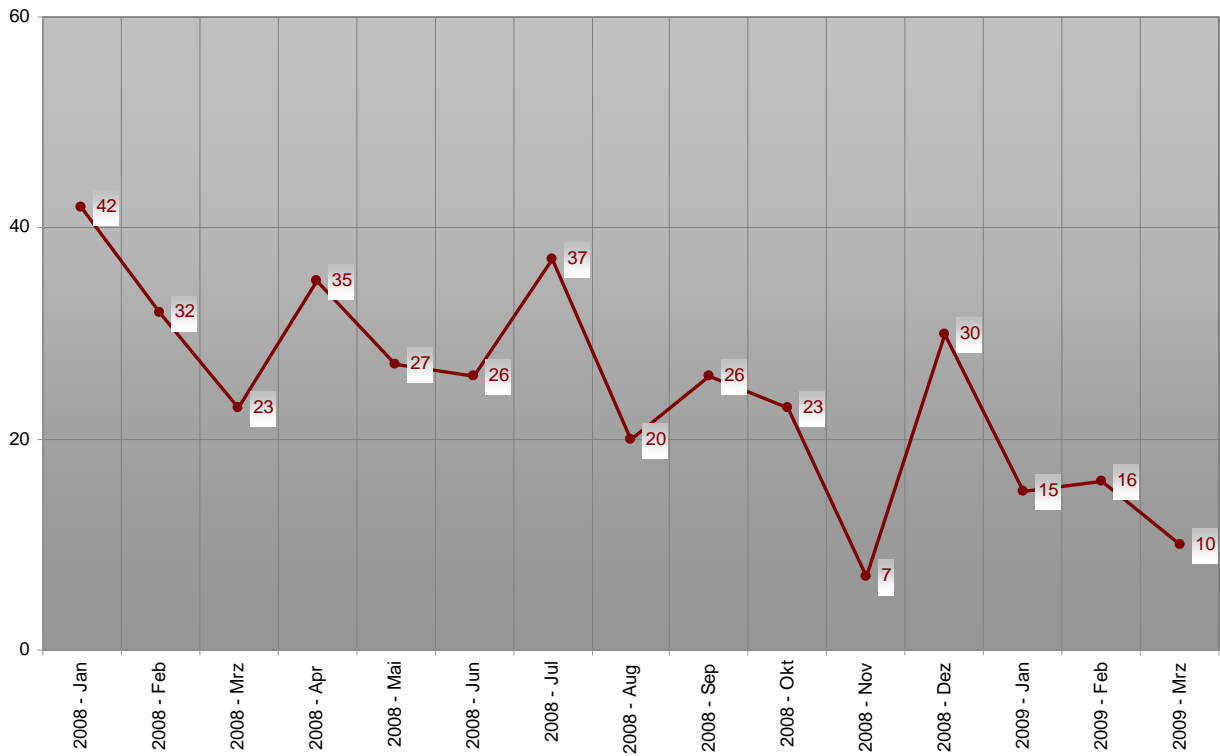


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

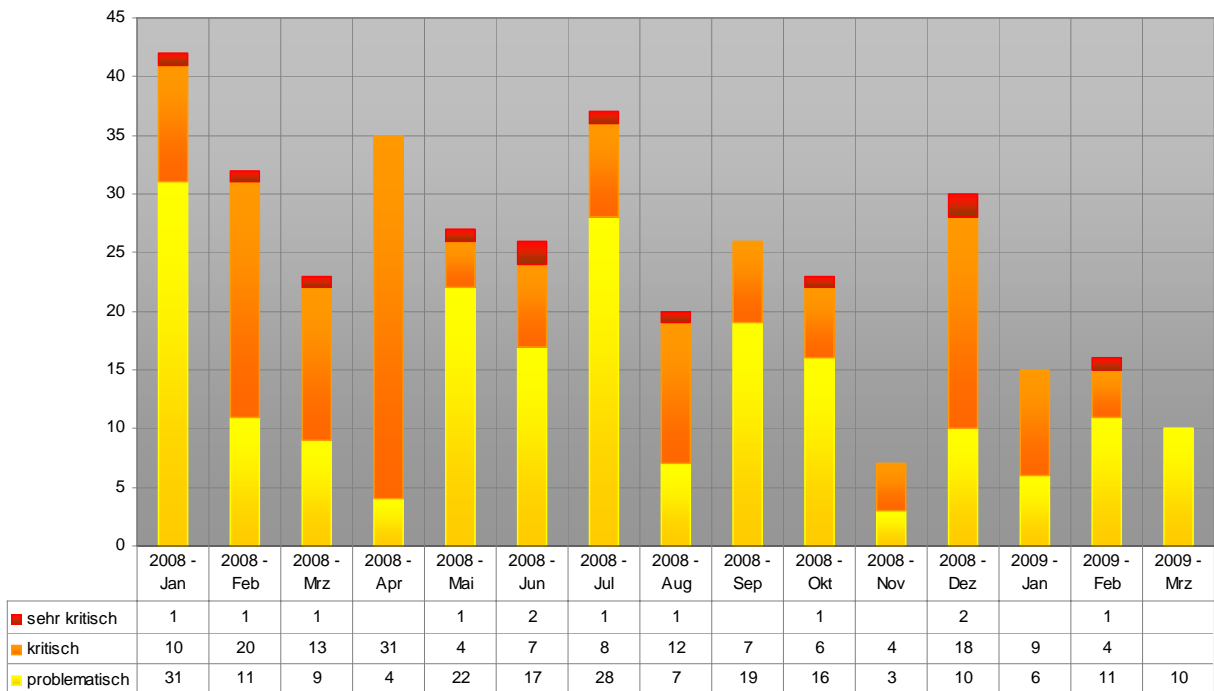


Verlauf der letzten drei Monate Schwachstelle/Kategorie

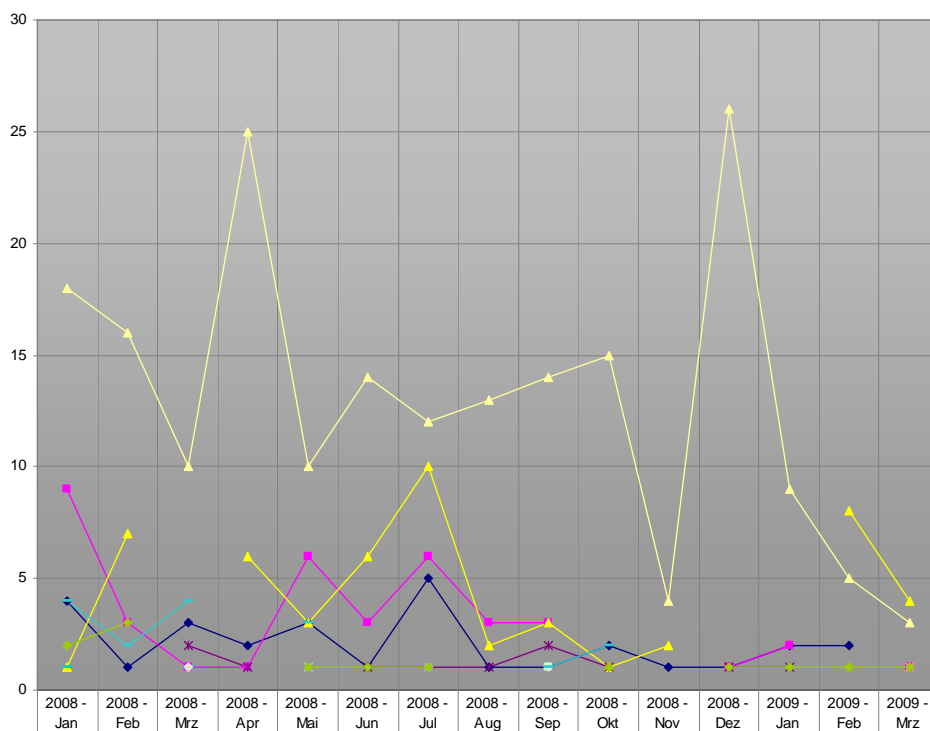
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008-2009



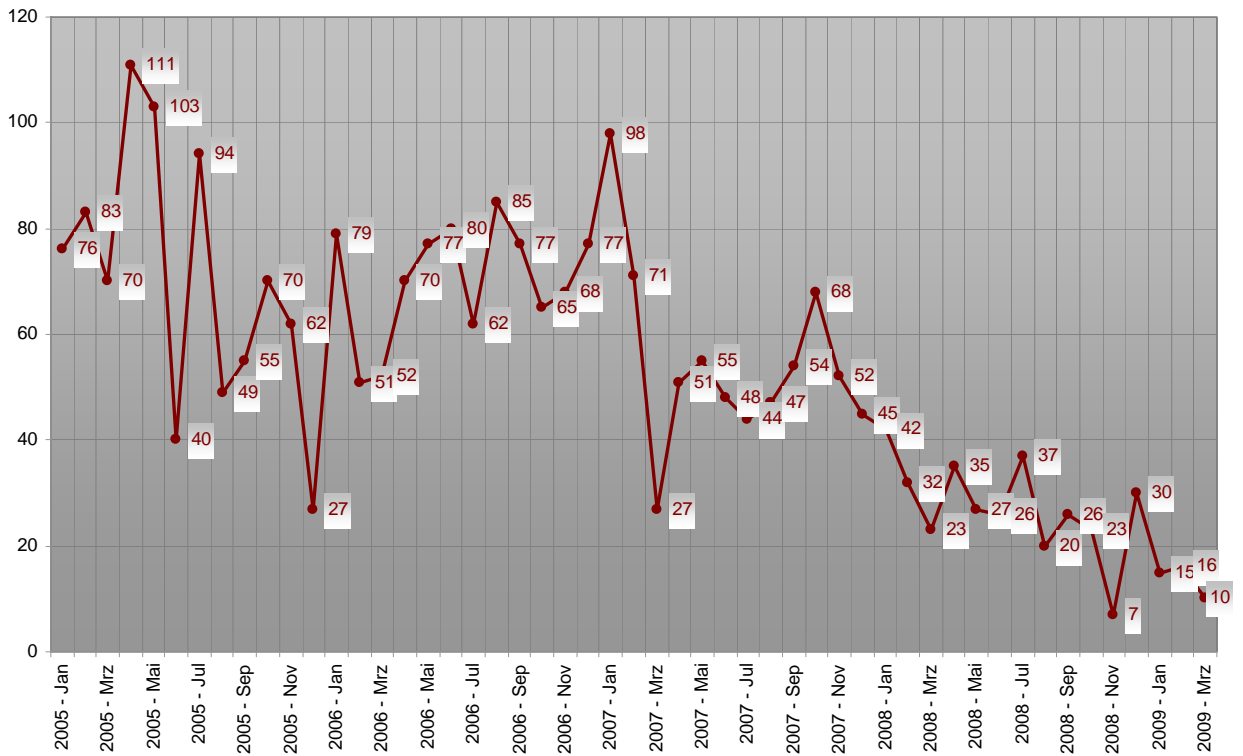
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2008-2009



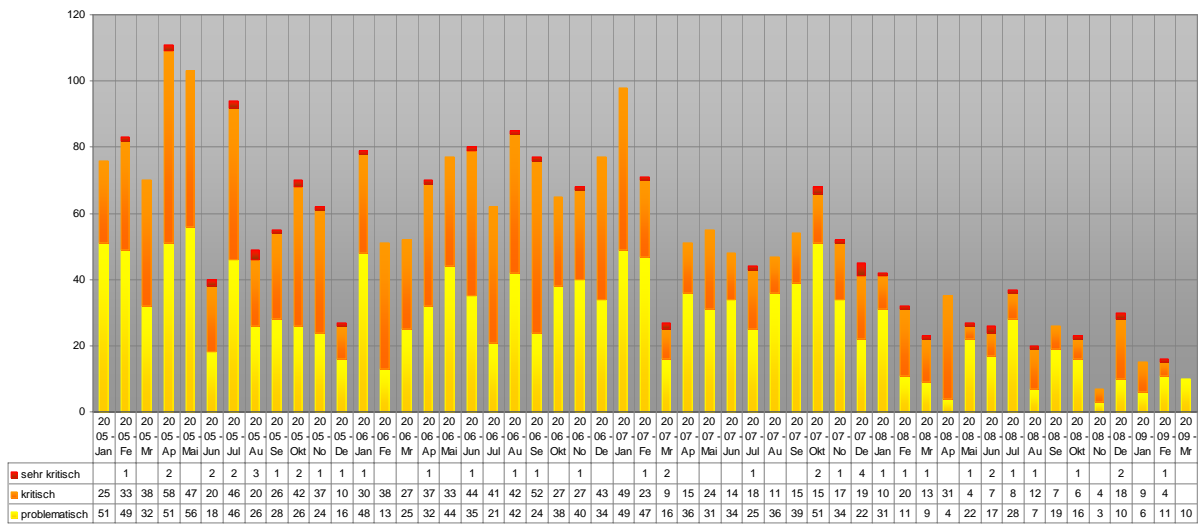
	2008 - Jan	2008 - Feb	2008 - Mrz	2008 - Apr	2008 - Mai	2008 - Jun	2008 - Jul	2008 - Aug	2008 - Sep	2008 - Okt	2008 - Nov	2008 - Dez	2009 - Jan	2009 - Feb	2009 - Mrz
◆ Cross Site Scripting (XSS)	4	1	3	2	3	1	5	1	1	2	1	1	2	2	
■ Denial of Service (DoS)	9	3	1	1	6	3	6	3	3			1	2		1
▲ Designfehler	1	7		6	3	6	10	2	3	1	2			8	4
✕ Directory Traversal															
✱ Eingabeungültigkeit			2	1		1	1	1	2	1		1	1		
● Fehlende Authentifizierung															
✚ Fehlende Verschlüsselung															
— Fehlerhafte Leserechte	1														
— Fehlerhafte Schreibrechte	1		1												
— Format String			1				1		1						
— Konfigurationsfehler									1						
▲ Pufferüberlauf	18	16	10	25	10	14	12	13	14	15	4	26	9	5	3
✕ Race-Condition					1		1								
✱ Schwache Authentifizierung															1
● Schwache Verschlüsselung															
— SQL-Injection	2		1							1					
— Symlink-Schwachstelle															
— Umgehungs-Angriff	4	2	4		3				1	2					

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2008-2009

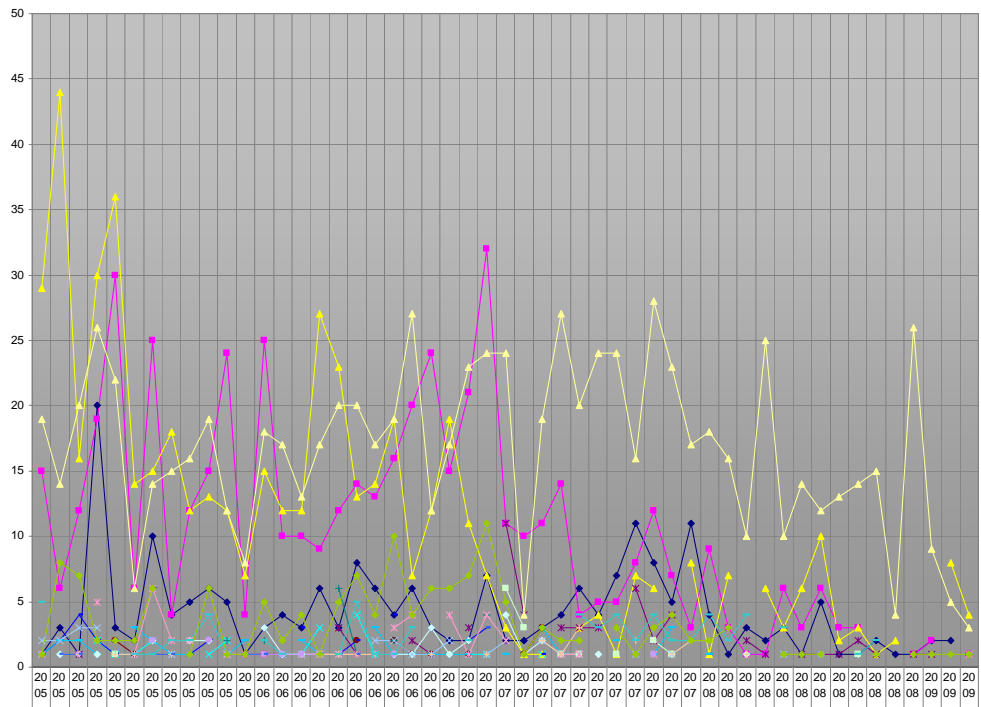
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005

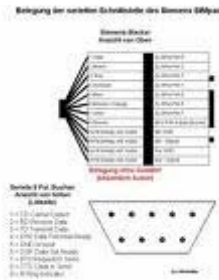


	2005-01	2005-02	2005-03	2005-04	2005-05	2005-06	2005-07	2005-08	2005-09	2005-10	2005-11	2005-12	2006-01	2006-02	2006-03	2006-04	2006-05	2006-06	2006-07	2006-08	2006-09	2006-10	2006-11	2006-12	2007-01	2007-02	2007-03	2007-04	2007-05	2007-06	2007-07	2007-08	2007-09	2007-10	2007-11	2007-12	2008-01	2008-02	2008-03	2008-04	2008-05	2008-06	2008-07	2008-08	2008-09	2008-10	2008-11	2008-12	2009-01							
◆ Cross Site Scripting (XSS)	1	3	1	20	3	2	10	4	5	6	5	1	3	4	3	6	3	8	6	4	6	3	2	2	7	2	2	3	4	6	4	7	11	8	5	11	4	1	3	2	3	1	5	1	1	2	1	1	2	2						
◆ Denial of Service (DoS)	15	6	12	19	30	6	25	4	12	15	24	4	25	10	10	9	12	14	13	16	20	24	15	21	32	11	10	11	14	4	5	5	8	12	7	3	9	3	1	1	6	3	6	3	3			1	2		1					
◆ Designfehler	29	44	16	30	36	14	15	18	12	13	12	7	15	12	12	27	23	13	14	19	7	12	19	11	7	3	1	1	3	4	1	7	6	8	1	7	6	3	6	10	2	3	1	2			8	4								
◆ Directory Traversal				2	1	1	2			1	2		1	1	1	3		4	1					1	1		1																													
◆ Eingabeungültigkeit		1			1							1	1	1		3	1		2	1	3	11	4	3	3	3	6	2	4								2	1	1	1	1	2	1		1	1										
◆ Fehlende Authentifizierung		1	2	1								1						2	2	1	1	1	1	1																																
◆ Fehlende Verschlüsselung				2		2	1	2		2	1	2	6	1	2		1	4					4																																	
◆ Fehlerhafte Leserechte	1	2	4	2	1	6	1	1	2		1	3	1	2		4						2	3		1																															
◆ Fehlerhafte Schreibrechte	1	2	2	1	3	2	1	1	1	2		2	1				3	1	1	1	1	1	1	1	1	1	3	1																												
◆ Format String	1		1		2	2	2				3	1	1	1																																										
◆ Konfigurationsfehler					1																																																			
◆ Pufferüberlauf	19	14	20	26	22	6	14	15	16	19	12	8	18	17	13	17	20	17	19	27	12	17	23	24	24	4	19	27	20	24	24	16	28	23	17	18	16	10	25	10	14	12	13	14	15	4	26	9	5	3						
◆ Race-Condition	2	2	3	3	1	1	1		1		1	1	1	1	1	2	2	1	1	2		1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1				
◆ Schwache Authentifizierung	1		5	1	6	2	2	1	1	1	1	1	1	1	1	1	3	4	4	1	4	2																																		
◆ Schwache Verschlüsselung	1		1			2	2																																																	
◆ SQL-Injection			1	1	1	1	1				1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	3																										
◆ Symlink-Schwachstelle	1	1	1	2	1	1	1				1	1	1	1	1	1																																								
◆ Umgehungs-Angriff	5				1	1	2	2	4	1	2	1		1	5	1	1	3																																						
◆ Unbekannt	1	8	7	2	2	6	1	6	1	1	5	2	4	1	5	7	4	10	4	6	6	7	11	5	1	3	2	2	3	1	3	4	2	2	3	1	3	4	2	2	3			1	1	1			1	1	1	1	1			

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat seit Januar 2005



5. Bilderrätsel



GESUCHTE BEGRIFFE		
9 (english)	6 (english)	3 (english)

LÖSUNGSWORT

scip monthly Security Summary 19.03.2009

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 **15.04.2009**. 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. Das **Errata** (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summaries finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)