

## Contents

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

### 1. Editorial

#### Unter Blinden wird auch der Einäugige nicht zwingend König

Ein Grossteil meiner Freunde und Bekannten sind oder waren Studenten. Seien dies nun Juristen, Soziologen oder Künstler. Für sie gelte ich, obschon mein Bildungsweg ganz anderes vermuten lässt, als Akademiker. Ich mag es, Probleme im Kopf zu lösen. So wie halt Sherlock Holmes auch. Und erscheint ein Sachverhalt dann mal zu komplex, greife ich zu "Papier und Bleistift". Je weniger ich mich bei einer Problemlösung bewegen muss, desto lieber habe ich das Problem. Das heisst aber nicht, dass ich mich nicht dabei dennoch bewege. Nietzsche sagte nicht umsonst, dass der Mensch im Gehen denkt.

Meine akademische Herangehensweise schlägt sich bei Sicherheitsüberprüfungen in der Hinsicht nieder, dass ich zu Beginn sämtliche Informationen zur Zielumgebung einsehen möchte. Dies umfasst jegliche Information, vom Grobkonzept über das Detailkonzept bis hin zu Produkt-Handbüchern und aktuellen Konfigurationseinstellungen. Also noch bevor ich

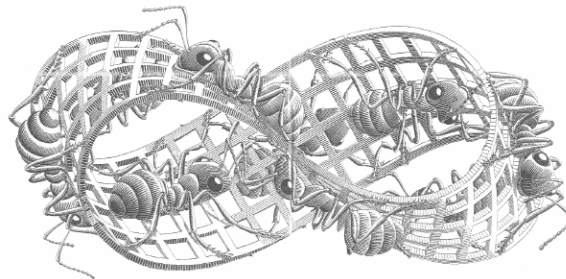
das erste IP-Datagramm über das Netzwerk jage, sollte ich eigentlich schon alles wissen, um keine unnötigen Zugriffe durchsetzen zu müssen. Im Idealfall habe ich das Zielsystem schon kompromittiert, noch bevor ich das RJ45-Kabel in meinen Laptop einstecke und meine VMwares hochfahre.

Eine solche systematische Deduktion ist vor allem dann von Vorteil, wenn man sich in sehr grossen und hochgradig komplexen Umgebungen zurechtzufinden hat. Viele Hosts, manchmal mit multiplen Schnittstellen und IP-Adressen sowie eine mehrschichtige Netzwerktopologie machen es gar unabdingbar, dass man sich als erstes auf dieser Ebene seiner Aufgabe nähert. Es ist deshalb schon fast Pflicht, dass der Kunde vorgängig die erforderlichen Daten sammelt und bereitstellt. Eine Aufgabe, die man nicht unterschätzen sollte.

Es ist Montag Morgen und ich melde mich beim Kunden an. Ich bin wie immer eine halbe Stunde zu früh. Heute ist nämlich mein erster Tag vor Ort und ich kann es nicht leiden, wenn ich zu spät komme. Das anstehende Projekt ist sehr zeitkritisch, denn so muss ich noch während der Aufbauphase einen Abnahmetest durchführen, so dass die neue Umgebung am Freitag der gleichen Woche in Betrieb gehen kann. Keine optimale Planung, ich weiss. Aber so ist das halt bei grossen Firmen. Es handelt sich dabei um eine hochsichere Single Sign-On Lösung (SSO):

Benutzer sollen sich einmal anmelden müssen und dann auf sämtliche Applikationen des Unternehmens zugreifen können. So fällt das Verwalten einer Unzahl an Zugangsdaten weg.

An der Testreihen Kickoff-Sitzung frage ich nach den Daten welche ich an der initialen Kick-Off Sitzung angefordert hatte: aktuelles Netzwerkschema sowie die IP-Adressen der Schnittstellen der involvierten Systeme (Reverse-Proxy, Alteon-Switches, WebSphere-Farm und Active Directory Server). Ohne diese Daten wird es nahezu unmöglich, dass ich im Wirrwar des Unternehmensnetzwerks die richtigen Systeme



angehe. Der für mich zuständige Herr gibt jedoch zu bedenken, dass die Chancen leider sehr gering sind, halbwegs aktuelle oder gar vollständige Informationen zu finden. Ich war etwas enttäuscht und gleichzeitig gespannt wann ich wohl die ersten Daten erhalten werde.

Zwischenzeitlich war ich mit dem Einrichten meines altertümlichen Dell-Laptops beschäftigt, als man mir mitteilte, dass es in der Tat keine Daten gibt. Kein Netzwerkschema. Keine IP-Adressen. "Doch, es gibt Adresslisten", sagt plötzlich jemand. Ich kriege fünf IP-Adressen zugesteckt. Welche wohin gehört, weiss niemand so richtig. Mittels ARP-Auflösungen und TTL-Auswertungen versuche ich Systeme zuzuordnen. Manche der Adressen gehören zu Clustern. Andere gehören zum gleichen Host, manchmal zur gleichen Schnittstelle. Es ist ein Chaos und ich der Einäugige im Land voller Blinder.

Abklärungen seien noch immer im Gange, versicherte man mir; auch am Tag darauf. Um nicht unnötig fortwährend in der Kaffeepause zu sitzen, versuche ich mal die klar eingegrenzten Systeme zu prüfen. Ich komme nicht richtig vorwärts. Um die Kerberos-Tickets zu analysieren, brauche ich Netzwerk-Sniffs der geschützten AD-Umgebung. Die kann ich nicht selber generieren, weshalb ich die Rückmeldung des Netzwerkteams abwarten muss. Dieses lässt sich Zeit. Und als dann mal jemand auf mich zukommt, so weiss er nicht genau, was ich will. Als ich ihm von SSO und WebSphere berichte meint er nur, dass niemand bei ihnen wisse, welche Hosts das seien. Das Chaos legt sich und vor mir steht das grosse Nichts. Der Begriff Nihilismus passt hier eigentlich ganz gut.

Ich kann nicht testen, da mir die grundlegendsten Informationen fehlen. Ohne Netzwerkdiagramme und IP-Adressen wird es unmöglich auszumachen, woher ich komme und wohin ich will. Der Test wird unterbrochen und ich lasse über die Projektleiter eskalieren. Die angestrebten Termine konnten natürlich nicht gehalten werden. Mein Resümee der letzten Tag war, dass diese Firma sich weniger Sorgen um Single Sign-On machen und die Kräfte lieber auf eine saubere Netzwerkdokumentation richten sollte. Davon hat man mehr. Und dann klappts auch mit dem nächsten Sicherheitstest.

Marc Ruff <maru-at-scip.ch>  
Security Consultant  
Zürich, 28. April 2008

## 2. scip AG Informationen

### 2.1 Web Application Penetration Test

Die Welt ohne Internet und ohne Webseiten ist nicht mehr vorstellbar. Keine Firma ohne Webaufritt! Die Ausprägung beginnt bei einfachen „Visitenkarten im Netz“ über interaktive Firmenvorstellungen mit notwendiger Softwareinstallation im Client-Browser bis hin zu komplexen Webapplikationen mit Datenbankanbindung 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!

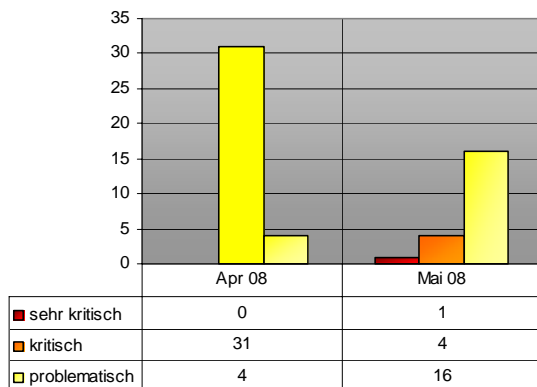
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an [chris.widmer@scip.ch](mailto:chris.widmer@scip.ch)

### 3. Neue Sicherheitslücken

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



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



#### Contents:

- 3711 Linux Kernel bis 2.6.25.1 fnctl() Race Condition
- 3710 Citrix Presentation Server unauthorisierter Zugriff
- 3709 Citrix Presentation Server schwache Kryptografie
- 3704 Debian OpenSSL vorhersagbare Zertifikatsgenerierung
- 3703 Citrix Access Gateway unspezifizierte Umgehung der Authentisierung
- 3702 Microsoft Publisher Object Handler Validation Schwachstelle
- 3701 Microsoft Word CSS Pufferüberlauf
- 3700 Microsoft Word RTF Objekt Pufferüberlauf
- 3699 Microsoft Windows CE Schwachstellen bei der Bildverarbeitung
- 3698 Internet Explorer "DisableCachingOfSSLPages" Schwachstelle
- 3693 PHP FastCGI Pufferüberlauf
- 3692 Linux Kernel bis 2.6.25.1 IPSEC ESP Denial of Service
- 3689 WordPress "cat" Directory Traversal Schwachstelle
- 3688 Adobe Produkte BMP Handling Pufferüberlauf
- 3687 ICQ Personal Status Pufferüberlauf bei Verarbeitung

### 3.1 Linux Kernel bis 2.6.25.1 fnctl() Race Condition

Einstufung: **problematisch**  
 Remote: Teilweise  
 Datum: 02.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3711>

Linux oder auch GNU/Linux (siehe GNU/Linux-Namensstreit) ist ein freies Multiplattform-Mehrbenutzer-Betriebssystem für Computer, das den Linux-Kernel verwendet, auf GNU basiert und Unix ähnlich ist. Erstmals in größerem Stil eingesetzt wurde Linux 1992 nach der GNU-GPL-Lizenzierung des Linux-Kernels. In aktuellen Versionen des Kernels existiert eine Schwachstelle, durch die ein Angreifer mittels fnctl() und close() eine Race Condition erzeugen kann die zum Absturz oder Applikation oder potentiell der Ausführung beliebigen Codes mit administrativen Privilegien führt,.

#### Expertenmeinung:

Auch der Linux Kernel wird wieder einmal mit einigen Schwachstellen bedacht, wenn auch diese nicht breitflächig ausgenutzt werden dürften. Der Zeitrahmen des Updates ist anhand einer angemessenen Risikoklassifizierung zu wählen, zumindest langfristig sollten diese Schwachstellen mittels eines Updates mitigiert werden.

### 3.2 Citrix Presentation Server unauthorisierter Zugriff

Einstufung: **problematisch**  
 Remote: Teilweise  
 Datum: 15.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3710>

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Der jetzige Präsident und CEO ist Mark B. Templeton. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CTXS gehandelt. Im Geschäftsjahr 2003 hat Citrix einen Umsatz von 588,6 Millionen US-Dollar erwirtschaftet. Im Jahr 2004 erreichte Citrix einen Umsatz von 741 Mio. US-Dollar. 2005 konnte der Umsatz auf 908 Mio. US-Dollar gesteigert werden, 2006 betrug der Umsatz 1,134 Mrd. US-Dollar. Im Citrix Presentation Server wurde eine Schwachstelle identifiziert, bei der ein unspezifizierter Fehler dazu führen kann, dass eine Desktop Session ohne die vorgängig notwendige Authentifizierung aufgebaut wird. Dadurch kann ein Angreifer unberechtigten



Zugriff auf Zielsysteme erlangen. Weitere Details wurden nicht bekanntgegeben.

#### Expertenmeinung:

Citrix bietet als verbreitete Lösung im Geschäftsumfeld einen wichtigen Angriffspunkt für professionelle Angreifer und ist von Natur aus in den meisten Konstellationen nicht gerade mit überdurchschnittlicher Sicherheit gesegnet. Die vorliegenden Schwachstellen lassen vermuten, dass der Höhepunkt der Angreifbarkeit hier noch nicht erreicht wurde. Leider hält sich der Hersteller mit Informationen zu den einzelnen Schwachstellen im Detail sehr bedeckt, was eine effiziente Einstufung schwierig bis unmöglich macht. Betroffene Administratoren sollten die entsprechenden Updates zeitnah einspielen.

### 3.3 Citrix Presentation Server schwache Kryptografie

Einstufung: **problematisch**  
 Remote: Teilweise  
 Datum: 15.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3709>

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Der jetzige Präsident und CEO ist Mark B. Templeton. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CCTX gehandelt. Im Geschäftsjahr 2003 hat Citrix einen Umsatz von 588,6 Millionen US-Dollar erwirtschaftet. Im Jahr 2004 erreichte Citrix einen Umsatz von 741 Mio. US-Dollar. 2005 konnte der Umsatz auf 908 Mio. US-Dollar gesteigert werden, 2006 betrug der Umsatz 1,134 Mrd. US-Dollar. Im Citrix Presentation Server wurde eine Schwachstelle identifiziert, durch deren Ausnutzung eine Verbindung etabliert werden kann, die eine tiefere Kryptografieeinstellung verwendet, als ursprünglich vorgesehen. So kann möglicherweise die Sicherheit dieser entsprechenden Verbindung soweit geschwächt werden, dass ein erfolgreicher Angriff möglich wird.

#### Expertenmeinung:

Citrix bietet als verbreitete Lösung im Geschäftsumfeld einen wichtigen Angriffspunkt für professionelle Angreifer und ist von Natur aus in den meisten Konstellationen nicht gerade mit überdurchschnittlicher Sicherheit gesegnet. Die vorliegenden Schwachstellen lassen vermuten, dass der Höhepunkt der Angreifbarkeit hier noch nicht erreicht wurde. Leider hält sich der Hersteller mit Informationen zu den einzelnen

Schwachstellen im Detail sehr bedeckt, was eine effiziente Einstufung schwierig bis unmöglich macht. Betroffene Administratoren sollten die entsprechenden Updates zeitnah einspielen.

### 3.4 Debian OpenSSL vorhersagbare Zertifikatsgenerierung

Einstufung: **sehr kritisch**  
 Remote: Ja  
 Datum: 13.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3704>

Debian GNU/Linux ist eine freie GNU/Linux-Distribution. Debian GNU/Linux enthält eine große Auswahl an Anwendungsprogrammen und Werkzeugen, zusammen mit Linux als Kernel. Daneben existierten auch Varianten mit anderen Kernen. Die aktuelle stabile Version, Debian Etch (4.0r3) genannt, wurde am 17. Februar 2008 veröffentlicht. In verschiedenen Distributionsversionen wurde festgestellt, dass aufgrund eines vor längerer Zeit eingespielten Patches die Sicherheit von OpenSSL Schlüsseln, wie sie zum Beispiel mit HTTP over TLS oder auch bei SSH Verbindungen genutzt werden nicht mehr gewährleistet ist. Defakto wurde dadurch die Vorhersagbarkeit der entsprechenden Schlüssel geschaffen.

#### Expertenmeinung:

Gerade für eine dermassen traditionsreiche und auch renommierte Distribution wie Debian dürfte dieser Vorfall natürlich pures Gift darstellen. So entwickelte sich dann auch der absehbare Flamewar zwischen OpenSSL-Team und Debian Maintainern in schier abstruser Weise. Administratoren sei geraten, sich aus den Scharmützeln herauszuhalten und stattdessen die Sicherheit Ihrer Server wiederherzustellen, indem sie eine aktuellere, als sicher zu betrachtende OpenSSL Version installieren und gegebenenfalls unsichere Schlüsselpaare austauschen.

### 3.5 Citrix Access Gateway un spezifizierte Umgehung der Authentisierung

Einstufung: **problematisch**  
 Remote: Ja  
 Datum: 13.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3703>

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Der jetzige

Präsident und CEO ist Mark B. Templeton. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CTXS gehandelt. Im Geschäftsjahr 2003 hat Citrix einen Umsatz von 588,6 Millionen US-Dollar erwirtschaftet. Im Jahr 2004 erreichte Citrix einen Umsatz von 741 Mio. US-Dollar. 2005 konnte der Umsatz auf 908 Mio. US-Dollar gesteigert werden, 2006 betrug der Umsatz 1,134 Mrd. US-Dollar. Im Citrix Presentation Server wurde eine Schwachstelle identifiziert, bei der ein unspezifizierter Fehler dazu führen kann, dass eine Desktop Session ohne die vorgängig notwendige Authentifizierung aufgebaut wird. Dadurch kann ein Angreifer unberechtigten Zugriff auf Zielsysteme erlangen. Weitere Details wurden nicht bekanntgegeben.

#### Expertenmeinung:

Citrix bietet als verbreitete Lösung im Geschäftsumfeld einen wichtigen Angriffspunkt für professionelle Angreifer und ist von Natur aus in den meisten Konstellationen nicht gerade mit überdurchschnittlicher Sicherheit gesegnet. Die vorliegenden Schwachstellen lassen vermuten, dass der Höhepunkt der Angreifbarkeit hier noch nicht erreicht wurde. Leider hält sich der Hersteller mit Informationen zu den einzelnen Schwachstellen im Detail sehr bedeckt, was eine effiziente Einstufung schwierig bis unmöglich macht. Betroffene Administratoren sollten die entsprechenden Updates zeitnah einspielen.

### 3.6 Microsoft Publisher Object Handler Validation Schwachstelle

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 13.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3702>

Microsoft Office Publisher ist neben Programmen wie Word, PowerPoint oder Excel im Office-Paket von Microsoft enthalten. Durch Vorlagen lassen sich Inhalte im WYSIWYG-Verfahren schnell und einfach veröffentlichen. Jedoch erreicht Publisher nicht die Komplexität von Layoutprogrammen wie Adobe InDesign oder QuarkXPress. Durch einen Fehler im Parsing von Object Handler Headerdaten kann ein Pufferüberlauf erzeugt und die Ausführung beliebigen Codes ermöglicht werden.

#### Expertenmeinung:

Publisher ist nicht unbedingt die populärste Applikation in Microsofts Officepaket, genießt aber dennoch eine hohe Verbreitung. Entsprechende Umgebungen, die Publisher zu ihrem Standardinventar zählen, sollten den entsprechenden Patch zeitnah einspielen.

### 3.7 Microsoft Word CSS Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 13.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3701>

Microsoft Word (oft auch kurz MS Word oder Word genannt) ist ein Textverarbeitungsprogramm der Firma Microsoft für die Windows-Betriebssysteme und Mac OS. Es ist Teil der Officesuite Microsoft Office sowie der auf private Nutzer zugeschnittenen Programmsammlung Microsoft Works Suite, wird aber auch einzeln verkauft. Durch das Parsing von CSS (Cascading Style Sheets) Werten in entsprechenden Direktiven kann ein Pufferüberlauf erzeugt und beliebiger Code zur Ausführung gebracht werden.

#### Expertenmeinung:

Sowohl das ZDI als auch iDefense veröffentlichten diesen Monat jeweils eine Schwachstelle, die das Ausführen von Code durch Microsoft Word erlaubt. Als Standardapplikation ist Word seit jeher ein sehr beliebtes Ziel, wodurch diese Lücken ernstgenommen und baldmöglichst durch das Einspielen entsprechender Patches mitigiert werden sollten.

### 3.8 Microsoft Word RTF Objekt Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 13.05.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3700>

Microsoft Word (oft auch kurz MS Word oder Word genannt) ist ein Textverarbeitungsprogramm der Firma Microsoft für die Windows-Betriebssysteme und Mac OS. Es ist Teil der Officesuite Microsoft Office sowie der auf private Nutzer zugeschnittenen Programmsammlung Microsoft Works Suite, wird aber auch einzeln verkauft. Durch einen Fehler im Parsing von Rich Text Objekten kann ein Pufferüberlauf entstehen, der die Ausführung beliebigen Codes erlaubt.

#### Expertenmeinung:

Sowohl das ZDI als auch iDefense veröffentlichten diesen Monat jeweils eine Schwachstelle, die das Ausführen von Code durch Microsoft Word erlaubt. Als Standardapplikation ist Word seit jeher ein sehr beliebtes Ziel, wodurch diese Lücken

ernstgenommen und baldmöglichst durch das Einspielen entsprechender Patches mitigiert werden sollten

### 3.9 Microsoft Windows CE Schwachstellen bei der Bildverarbeitung

Einstufung: **kritisch**  
Remote: Ja  
Datum: 12.05.2008  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3699>

Windows CE, oft auch als WinCE abgekürzt, ist eine Familie von Betriebssystemen von Microsoft für PDA und embedded Systems. Es ähnelt in der Bedienung MS-Windows für PCs, verwendet aber einen anderen Kernel. Somit funktionieren auch keine herkömmlichen Windows-Programme. CE unterstützt die Prozessorarchitekturen Intel x86, MIPS, ARM (mit Intel PXA) und Hitachi SuperH. Es kann auch als hartes Echtzeitbetriebssystem eingesetzt werden. Microsoft bestätigte unlängst eine Schwachstelle in der Verarbeitung von Bilddateien, die zu einem Pufferüberlauf führen kann und die Ausführung beliebigen Codes ermöglicht.

#### Expertenmeinung:

Mobile Systeme dienen immer häufiger als Ziele für wohldurchdachte Angriffe auf Unternehmensnetzwerke. Hier sollte daher besondere Aufmerksamkeit aufgebaut werden. Es gilt, die freigegebenen Patches analog üblicher Systeme zeitnah zu installieren.

### 3.10 Internet Explorer "DisableCachingOfSSLPages" Schwachstelle

Einstufung: **problematisch**  
Remote: Teilweise  
Datum: 12.05.2008  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3698>

Windows Internet Explorer (früher Microsoft Internet Explorer, Abkürzung: IE oder auch MSIE) bezeichnet einen Webbrowser von Microsoft für das Betriebssystem Microsoft Windows. Seit Windows 95b, SR2 ist der Internet Explorer fester Bestandteil von Windows-Betriebssystemen. Bei älteren Windows-Versionen kann er nachinstalliert werden. Den „Microsoft Internet Explorer“ gab es für einige Zeit auch Versionen für Mac OS und Unix-Derivate (wie Solaris und HP-UX). Die derzeit

aktuelle Version ist Windows Internet Explorer 7. Bill Knox beschreibt in einem Advisory eine fehlerhafte Verhaltensweise, wonach die Option "DisableCachingOfSSLPages" nicht korrekt funktioniert. Der Sinn dieser Option wäre es, dass verschlüsselt übertragenen Seiten nicht auf die Festplatte des Benutzers geschrieben werden. Defakto scheint dies aber nicht korrekt implementiert worden zu sein. Dadurch können vertrauliche Daten auf der Festplatte des Benutzers über längere Zeit hinweg auffindbar sein.

#### Expertenmeinung:

Microsofts Internet Explorer zeigte sich in den letzten Monaten erstaunlich resistent gegenüber markanten Schwachstellen. Statistisch gesehen war die vorliegende Lücke also zu erwarten. Obschon diese nicht als kritisch anzusehen ist, sollte ein allfällig erscheinender Patch aufgrund der hohen Verbreitung des Produktes zeitnah eingespielt werden.

### 3.11 PHP FastCGI Pufferüberlauf

Einstufung: **problematisch**  
Remote: Ja  
Datum: 02.05.2008  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3693>

PHP (rekursives Backronym für „PHP: Hypertext Preprocessor“, ursprünglich „Personal Home Page Tools“) ist eine Skriptsprache mit einer an C bzw. C++ angelehnten Syntax, die hauptsächlich zur Erstellung von dynamischen Webseiten oder Webanwendungen verwendet wird. In Versionen vor 5.2.6 wurde eine Schwachstelle gemeldet, bei der ein un spezifizierter Fehler in der FastCGI SAPI zu einem stackbasierten Pufferüberlauf führen kann.

#### Expertenmeinung:

Als populäre Skriptsprache bietet PHP natürlich einen besonderen Reiz, ist doch die Verbreitung auf allgemein öffentlich zugänglichen System sehr hoch und entsprechend eine hohe Menge an Zielsystemen vorhanden. Die hier besprochenen Schwachstellen sind gesamthaft als problematisch einzustufen und sollten auf betroffenen Systemen durch ein baldiges Update auf eine neuere Version behoben werden.

### 3.12 Linux Kernel bis 2.6.25.1 IPSEC ESP Denial of Service

Einstufung: **problematisch**  
Remote: Teilweise  
Datum: 02.05.2008  
scip DB: <http://www.scip.ch/cgi->

bin/smss/showadvf.pl?id=3692

Linux oder auch GNU/Linux (siehe GNU/Linux-Namensstreit) ist ein freies Multiplattform-Mehrbenutzer-Betriebssystem für Computer, das den Linux-Kernel verwendet, auf GNU basiert und Unix ähnlich ist. Erstmals in größerem Stil eingesetzt wurde Linux 1992 nach der GNU-GPL-Lizenzierung des Linux-Kernels. In aktuellen Versionen des Kernels existiert eine Schwachstelle, bei der durch einen Fehler in der Implementierung von IPSec, genau genommen in der Behandlung von ESP Paketen, ein Denial of Service erzeugt werden kann.

#### Expertenmeinung:

Auch der Linux Kernel wird wieder einmal mit einigen Schwachstellen bedacht, wenn auch diese nicht breitflächig ausgenutzt werden dürften. Der Zeitrahmen des Updates ist anhand einer angemessenen Risikoklassifizierung zu wählen, zumindest langfristig sollten diese Schwachstellen mittels eines Updates mitigiert werden.

### 3.13 WordPress "cat" Directory Traversal Schwachstelle

Einstufung: **problematisch**  
 Remote: Ja  
 Datum: 25.04.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3689>

WordPress ist ein Weblog-Publishing-System (auch CMS), das vorwiegend bei der Erstellung von häufig zu aktualisierenden Websites, im Besonderen von Weblogs, eingesetzt wird. Es basiert auf der Skriptsprache PHP und benötigt eine MySQL-Datenbank. WordPress ist Freie Software, die unter der GNU General Public License lizenziert wurde. Die quelloffene Software stellen die Programmierer auf der Website kostenlos zum Download bereit. Die Entwickler von WordPress legen besonderen Wert auf Webstandards, Eleganz, Benutzerfreundlichkeit und leichte Anpassbarkeit der Software. Sandor Attila Gerendi fand eine Schwachstelle in der aktuellen Version 2.5.0, bei der durch die fehlender Validierung des Parameters "cat" eine Directory Traversal Attacke möglich wird. Dadurch kann ein Angreifer möglicherweise Zugriff auf vertrauliche Daten gewinnen.

#### Expertenmeinung:

Und wieder einmal ist es soweit: Nachdem die neue Version 2.5.0 als Lösung aller Problem angesehen wurde, erfolgt hier die Rückkehr auf den (harten) Boden der Tatsache. Gleich zwei

neue Schwachstellen mit problematischen bis kritischen Ausmassen gibt es zu verzeichnen. Geplagten Administratoren sei das Einspielen des Updates auf 2.5.1 empfohlen.

### 3.14 Adobe Produkte BMP Handling Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 22.04.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3688>

Adobe Systems ist ein US-amerikanisches Softwareunternehmen. Es wurde 1982 von John Warnock und Charles Geschke, den Erfindern des Dokumentenformats PostScript, gegründet. Der Name Adobe (span. Lehmziegel, von „adobar“ eingipsen) leitet sich von einem Fluss namens Adobe Creek ab, der hinter dem Haus eines der Gründer des Unternehmens verläuft. Wie Scott Laurie berichtet, kann mittels eines speziell manipulierten Bitmaps ein Pufferüberlauf provoziert werden, der die Ausführung beliebigen Codes auf dem Zielsystem erlaubt.

#### Expertenmeinung:

Aus den Informationen des Advisories und auch des Herstellers geht nicht abschliessend klar hervor, welche Produkte und Versionen betroffenen sind. Bestätigt sind Adobe Photoshop Album Starter Edition 3.2 und Adobe After Effects CS3. Wer andere, vergleichbare Produkte einsetzt sollte auch dort bemüht sein, allfällig spontan erscheinende Sicherheitsupdates zeitnah einzuspielen.

### 3.15 ICQ Personal Status Pufferüberlauf bei Verarbeitung

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 21.04.2008  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3687>

ICQ (Homophon für „I seek you“, zu deutsch „Ich suche dich“) ist ein Instant-Messaging-Programm von AOL. Benutzer können damit über das Internet miteinander chatten oder zeitversoben Nachrichten versenden. Zusammen mit dem AOL Messenger hatte ICQ im Oktober 2005 mit 56 % Marktanteil die Marktführerschaft im Bereich Instant Messaging. Das verwendete proprietäre Netzwerkprotokoll heißt OSCAR. Durch einen, von Leon Juranic, gefundenen Fehler kann ein Angreifer einen heap-basierten Pufferüberlauf durch das Setzen eines bestimmten Personal Status erreichen. Dies

erlaubt die Ausführung beliebigen Codes auf entsprechenden Gegenstellen.

**Expertenmeinung:**

Wie schon oft an dieser Stelle erwähnt, genießen Instant Messaging Applikationen ein ganz besonderes Interesse spezifischer Angreifergruppen, die zum Beispiel am Aufbau oder der Erweiterung eines Botnets interessiert sind. ICQ als "Big Player" in diesem Marktsegment dürfte das eigentlich mittlerweile wissen und die vorliegende Lücke ernstnehmen. Es empfiehlt sich daher, das freigegebene Update zu installieren um diese Schwachstelle zu beheben.

## 4. Statistiken Verletzbarkeiten

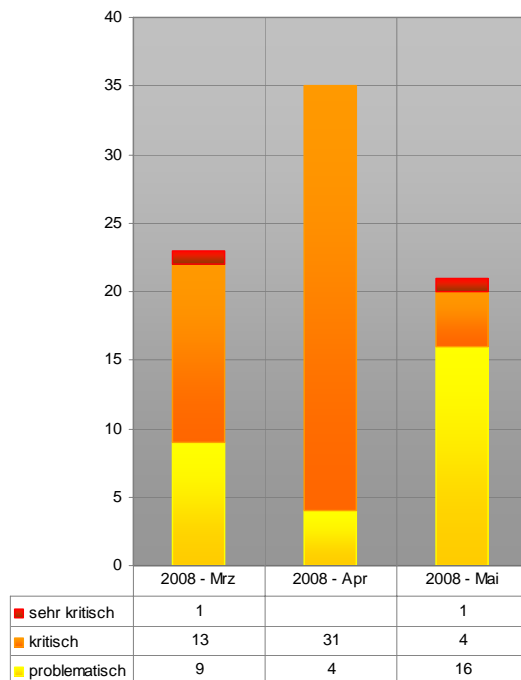
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



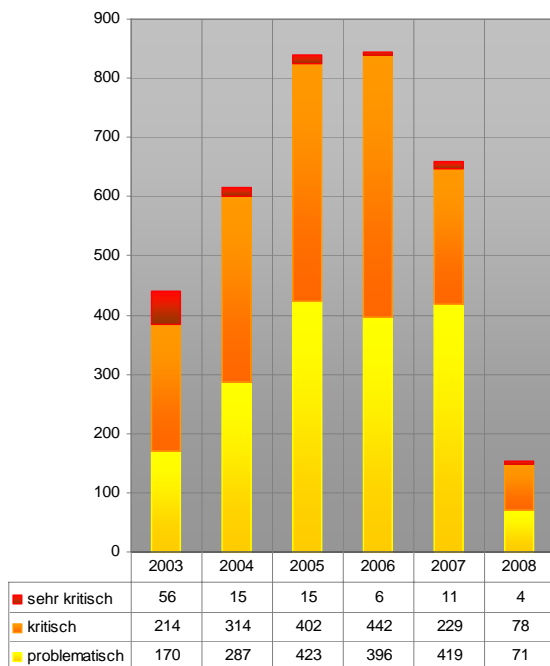
<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

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.

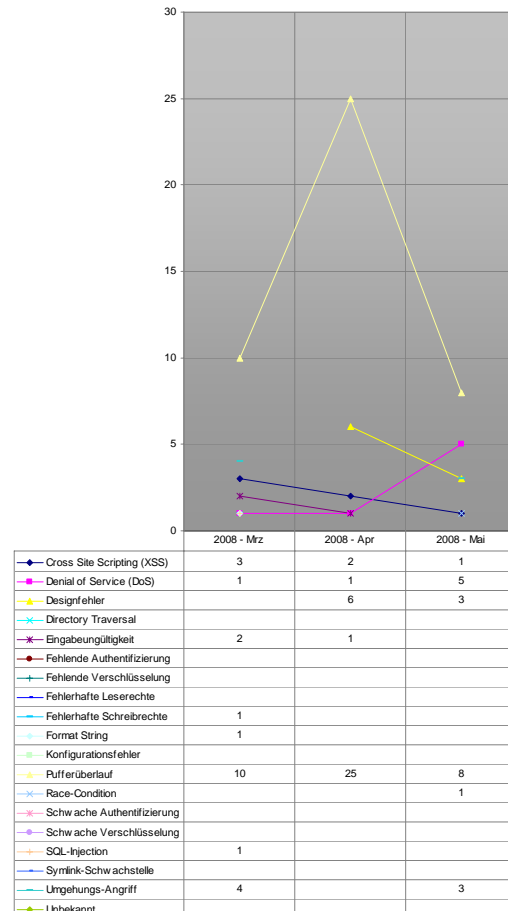
Auswertungsdatum: 19. Mai 2008



Verlauf der Anzahl Schwachstellen pro Jahr

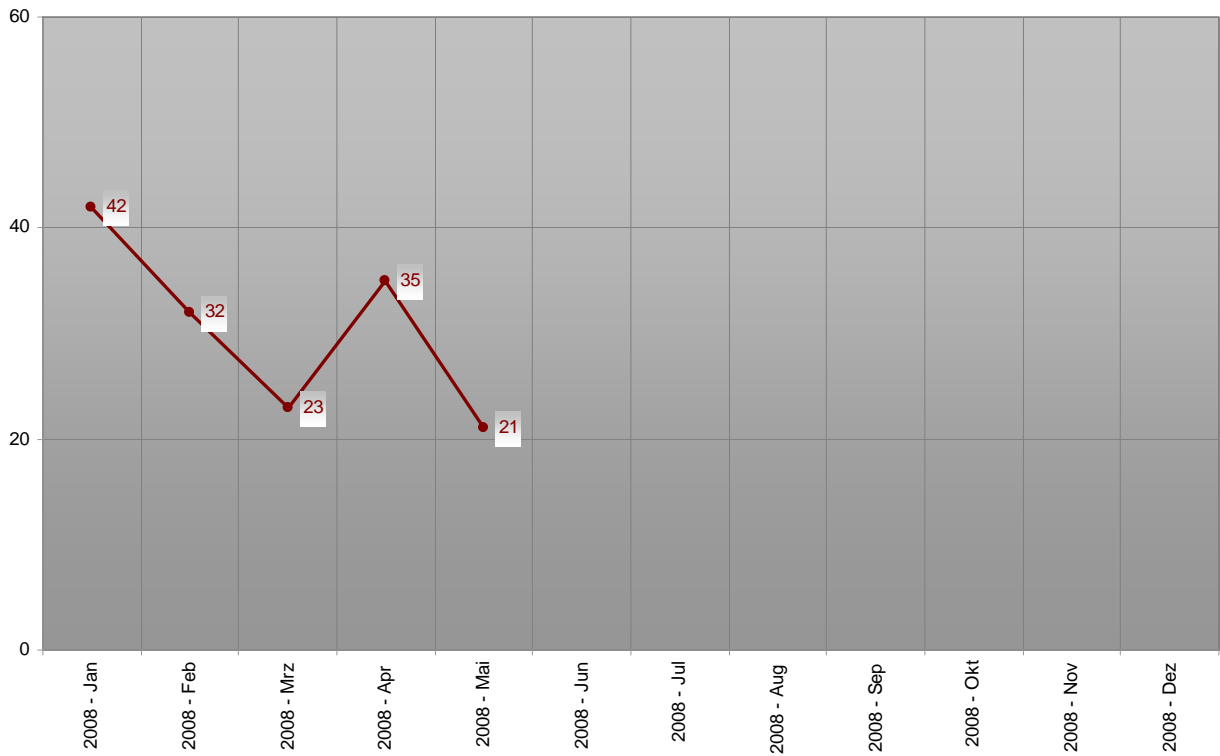


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

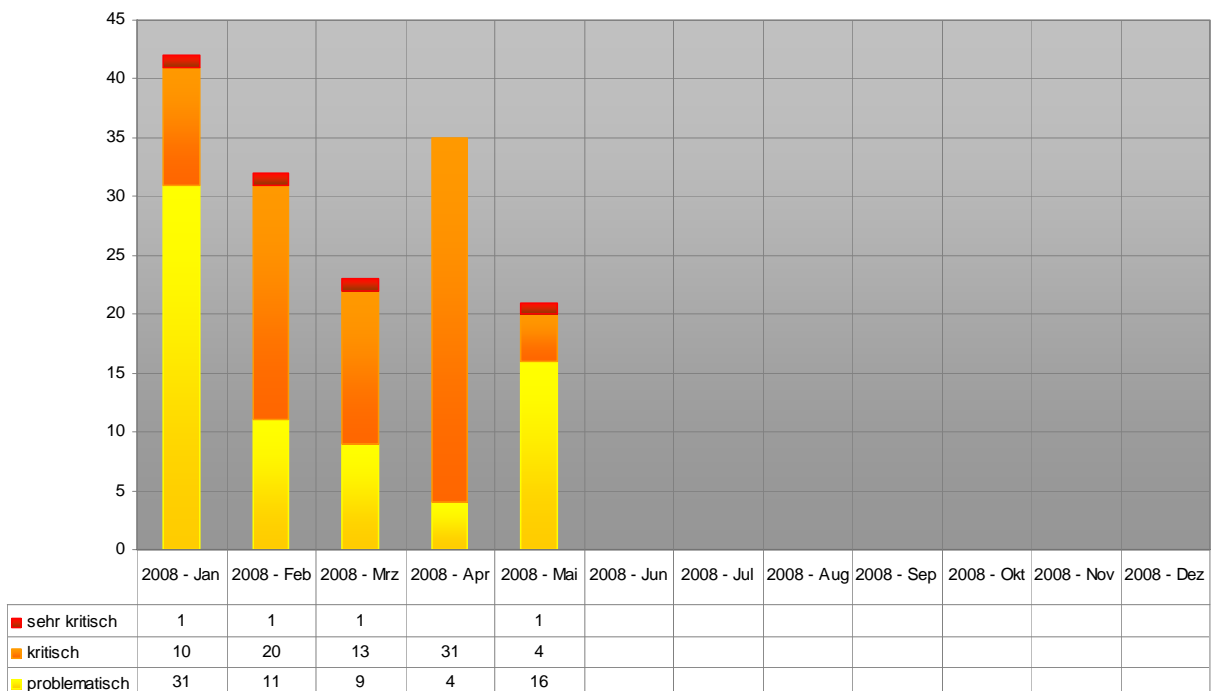


Verlauf der letzten drei Monate Schwachstelle/Kategorie

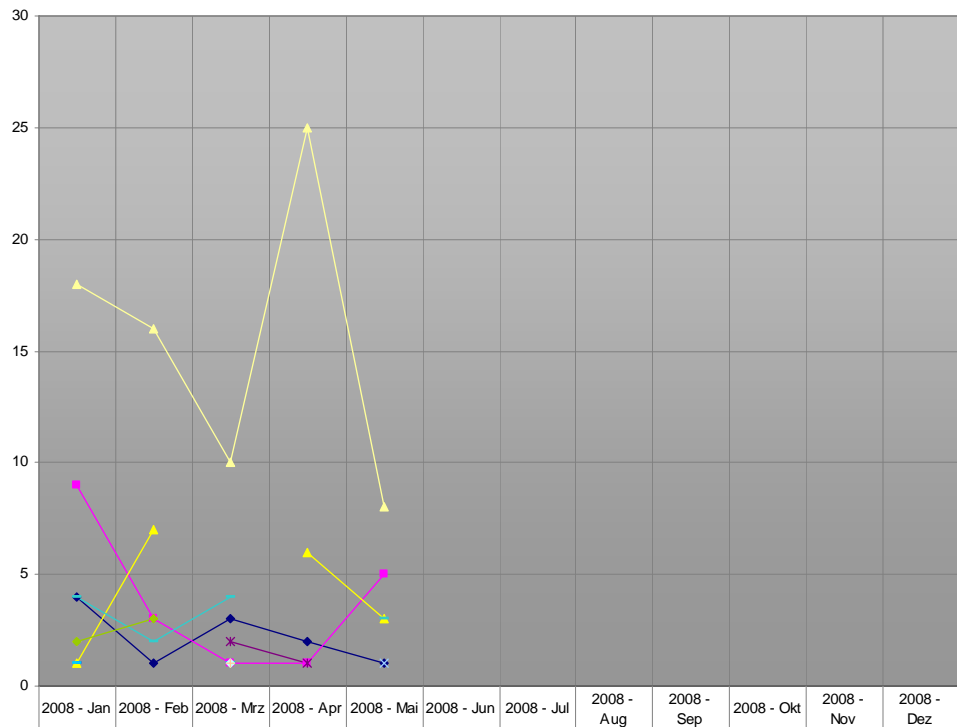
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008



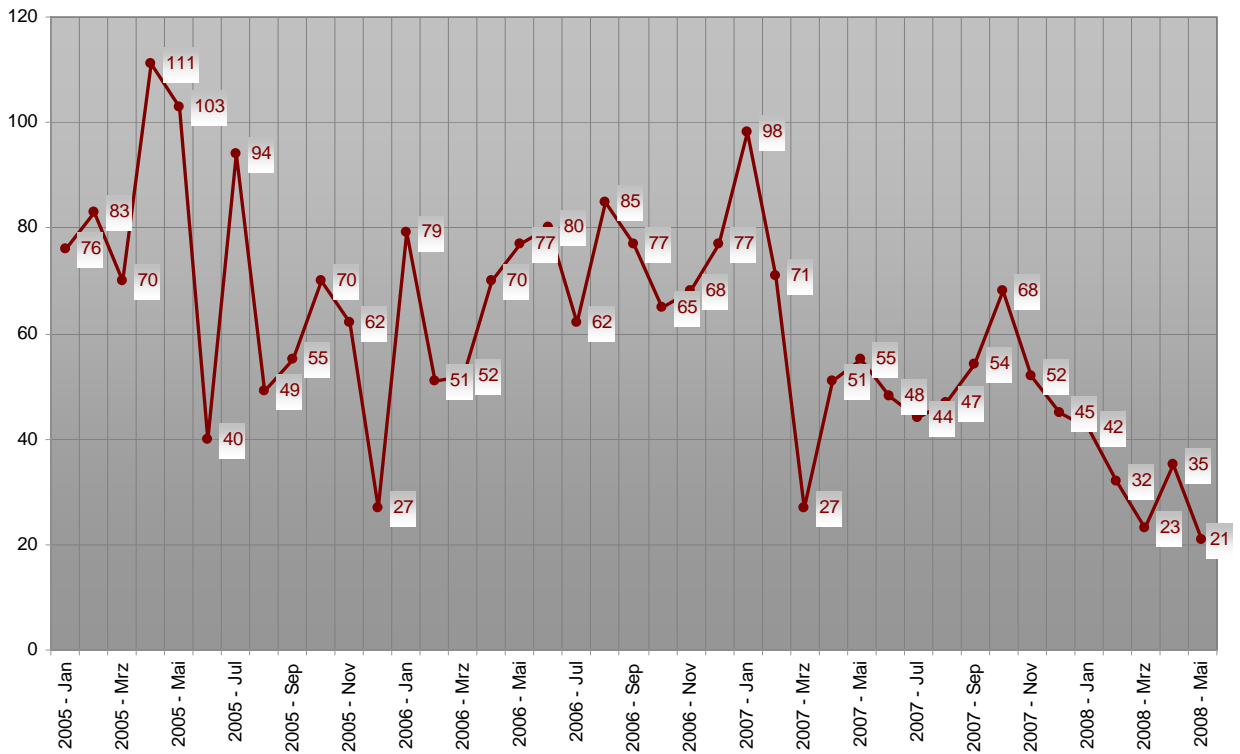
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2008



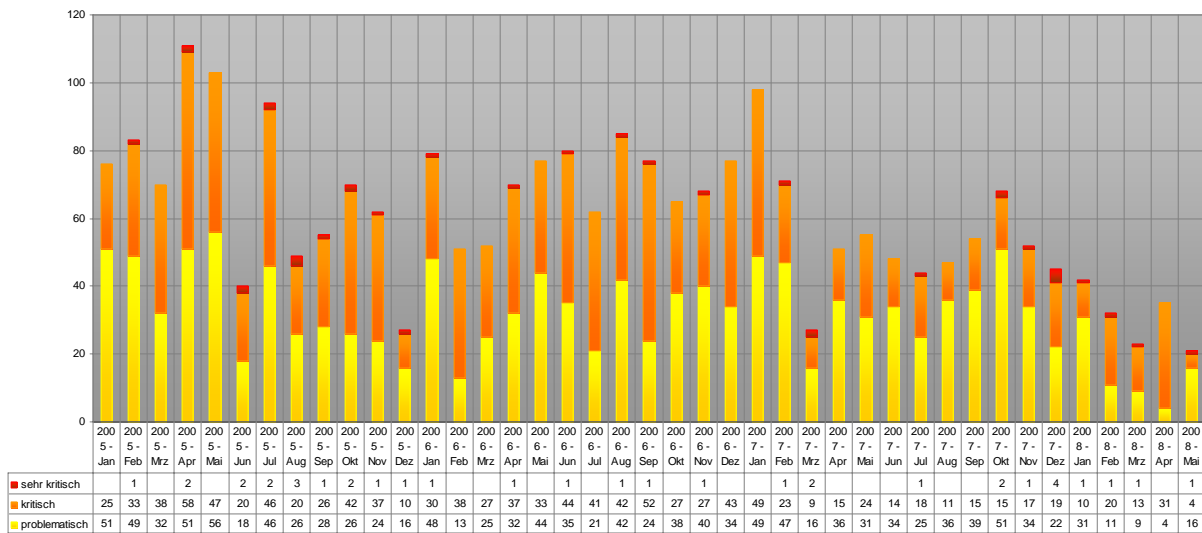
	2008 - Jan	2008 - Feb	2008 - Mrz	2008 - Apr	2008 - Mai	2008 - Jun	2008 - Jul	2008 - Aug	2008 - Sep	2008 - Okt	2008 - Nov	2008 - Dez
◆ Cross Site Scripting (XSS)	4	1	3	2	1							
◆ Denial of Service (DoS)	9	3	1	1	5							
▲ Designfehler	1	7		6	3							
◆ Directory Traversal												
◆ Eingabeungültigkeit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

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2008

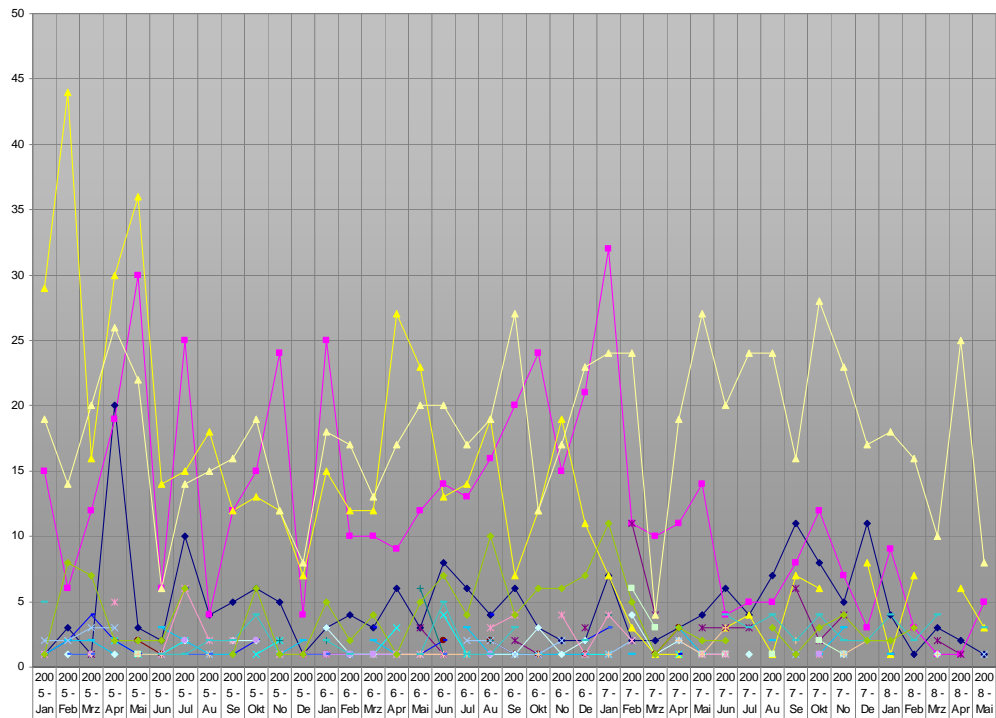
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005



	2005-1	2005-2	2005-3	2005-4	2005-5	2005-6	2005-7	2005-8	2005-9	2005-10	2005-11	2005-12	2006-1	2006-2	2006-3	2006-4	2006-5	2006-6	2006-7	2006-8	2006-9	2006-10	2006-11	2006-12	2007-1	2007-2	2007-3	2007-4	2007-5	2007-6	2007-7	2007-8	2007-9	2007-10	2007-11	2007-12	2008-1	2008-2	2008-3	2008-4	2008-5		
◆ 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	1		
◆ 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	5		
◆ 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	1	3			
◆ Directory Traversal				2	1	1	2			1	2		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			
◆ Fehlende Authentifizierung			1	2	1							1				2	2	1	1	1			1																				
◆ Fehlende Verschlüsselung					2		2		1		2		2		1	6	1		2			1		4																			
◆ Fehlerhafte Leserechte	1	2	4	2	1		6		1	2			1	3	1	2			4				2	3			1												1				
◆ Fehlerhafte Schreibrechte	1	2	2	1		3	2	1	1		1	2			2	1			3	1	1	1	1	1	1	1	1	3	1					2		1	3		1	1			
◆ Format String		1		1			2		2	2			3	1	1	1				1	1	3	1	2		4	1	2				1									1		
◆ Konfigurationsfehler					1																				6	3		1	1														
◆ Pufferüberlauf	19	14	20	26	22	6	14	15	16	19	12	8	18	17	13	17	20	20	17	19	27	12	17	23	24	24	4	19	27	20	24	24	16	28	23	17	18	16	10	25	8		
◆ Race-Condition	2	2	3	3		1	1			1			1	1	1			2	2	1	1	2		1	2		2	1	1					1		1						1	
◆ Schwache Authentifizierung	1			5		1	6	2	2		1	1	1	1	1	1	1	1	3	4		4	1	4	2			1	1														
◆ Schwache Verschlüsselung	1		1				2			2			1	1	1	1																											
◆ SQL-Injection				1	1	1	1		1				1	1	1	1						1			1			2	1	3				2	1	2	2	1					
◆ Symlink-Schwachstelle		1	1	2		1	1			1	1		1	1		1								3																			
◆ Umgehungs-Angriff	5					1	1	2	2	4	1		2	1				1	5	1	1	3		2						4	3	4	2	4	2	2	4	2	4	2	4	3	
◆ Unbekannt	1	8	7	2	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					

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat seit Januar 2005

## 5. Bilderrätsel



GESUCHTE BEGRIFFE		
8 Buchstaben (Name engl.)	5 Buchstaben (Name engl.)	3 Buchstaben

LÖSUNGSWORT

scip monthly Security Summary 19.05.2008

### 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 **15.06.2008**. 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 Ruef  
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!](#)