

Contents

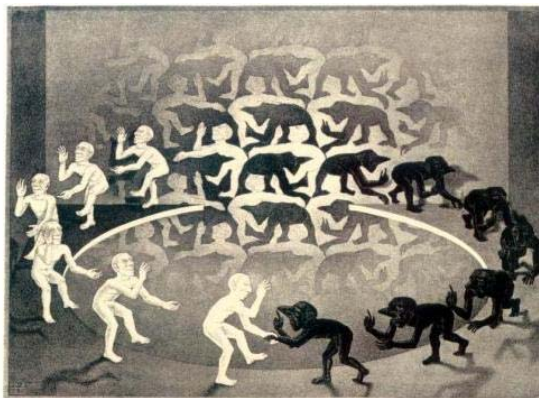
1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Statistiken Verletzbarkeiten
5. Bilderrätsel
6. Impressum

1. Editorial

Das Cookie ist mächtiger als das Schwert

Unsere Firma bietet verschiedene Module an, anhand derer wir die Sicherheit von Produkten, Lösungen und Installationen untersuchen können. Klassischerweise wird zum Beispiel ein Penetration Test auf eine Webapplikation durchgeführt, um typische Schwachstellen wie Cross Site scripting und SQL-Injection ausfindig zu machen.

Aufgrund verschiedener Automatismen sind wir ebenfalls besonders stark darin, wenn es um sogenannte Config Reviews geht. Sodann erhalten wir die Konfiguration eines Systems, Dienstes oder einer Applikation, die auf etwaige Schwächen hin untersucht werden soll. Der Grundlegende Ablauf gestaltet sich dabei stets gleich. Als erstes wird anhand des Handbuchs, durch Interviews mit Administratoren/Entwicklern oder einer allgemeinen Quelltext-Analyse die Funktionsweise und Möglichkeiten des Produkts angeschaut. Damit kann herausgefunden



werden, welche Funktionen und Einstellungen dargeboten werden.

In einem zweiten Schritt werden zu sämtlichen Möglichkeiten unsere generischen Wunschvorstellungen festgehalten. Unterstützt ein Webserver zum Beispiel SSL und wird das dedizierte Aktivieren unterschiedlicher Versionen angeboten, so sprechen wir uns für TLS/SSLv3 und gegen SSLv2 als empfohlene Einstellung aus.

Im dritten Schritt werden die applizierten Einstellungen mit unseren Wünschen verglichen. Jegliche Abweichung muss untersucht und spezifisch bewertet werden. Wird denn nun in einer Konfiguration die Generierung von Zufallszahlen mit /dev/random vorgesehen, äussern wir unsere Bedenken bezüglich der echten Zufälligkeit dieser Methode. Jenachdem wird ein solcher Punkt mit Low oder gar Medium (in Hochsicherheitsumgebungen) bewertet.

Mögliche und empfohlene Massnahmen werden dokumentiert, damit der Kunde eine Optimierung anstreben kann (z.B. Nutzung von /dev/random oder gar Einsatz eines echten Zufallszahlengenerators auf Hardwarebasis). Es bleibt sodann im Rahmen der klassischen Risikokalkulation dem Kunden überlassen, ob er das durch uns eruierte Risiko akzeptieren oder minimieren will. In jedem Fall muss man sich dessen bewusst sein und mit ihm umgehen können.

Vor einiger Zeit haben wir eine Config Review einer Reverse-Proxy Installation durchgeführt.

Dieser sollte im Rahmen meines Auftrags mehrere hundert Applikationen eines weltweit agierenden Unternehmens schützen. Jeglicher Zugriff aus dem Internet oder Intranet wurde über diese Komponente geschleust, um den traditionellen Common Point of Trust gewährleisten zu können. Dabei wurden beispielsweise die Grösse von POST-Anfragen, die Prüfung von Formularfeldern oder das

Verboten unerwünschter HTTP-Methoden durchgesetzt.

Mitunter sah das Produkt auf der Basis von Apache eine spezielle Funktion vor. Und zwar liess sich über eine ausgewählte Direktive bestimmen, wie sich das Regelwerk verhalten sollte, sollte der Benutzer mit einem definierten Cookie daherkommen. Zu meinem Erstaunen musste ich feststellen, dass gewisse "Debug-Cookies" vorgesehen waren, bei deren Nutzung sämtliche Sicherheitsfunktionen auf dem Proxy für diesen Benutzer temporär umgangen wurden.

Dies ist natürlich ein kritisches Problem. Schliesslich ist es einem Endanwender möglich, durch das simple Setzen eines Cookies die durch das Unternehmen auferlegte Sicherheitsrichtlinie zu umgehen. Mit dem Web Developer Plugin für Mozilla Firefox ist dies eine Sache von 3 Klicks. Die Mächtigkeit des Proxy-Elements wird damit gänzlich untergraben und die Sicherheit kann dadurch nicht mehr gewährleistet werden.

Die Entwickler und Administratoren argumentieren in diesen Fällen gerne, dass ein solches Debug-Cookie ja geheim sei (wie ein Passwort) und lediglich durch privilegierte Benutzer eingebracht werden sollte. Doch dies ist das klassische Problem der Security By Obscurity, denn spätestens beim Bekanntwerden des Cookie-Namens muss mit Missbräuchen gerechnet werden. Bei mehreren hundert Mitarbeitern in der IT-Abteilung, die von diesem Cookie wissen, wird wohl mit an 100 % grenzender Wahrscheinlichkeit irgendjemand - wenn auch erst nach seinem Weggang - einer Drittperson von dieser Hintertür erzählen. Eine virale Verbreitung dieser Information ist möglich, ja gar absehbar. Kann das Security-Team dann noch schnell genug reagieren, um das Cookie-Feature abzuschalten oder einen neuen "geheimen" Cookie-Namen zu vergeben?

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 20. April 2009

2. scip AG Informationen

2.1 Securing Citrix

Zentralisierte Lösungen wie Citrix erfreuen sich aufgrund sicherheitstechnischer und wirtschaftlicher Vorteile vor allem im professionellen Umfeld immer grösserer Beliebtheit.

Eine derartig umfassende Multiuser-Umgebung birgt ein erhebliches Risikopotential in sich welches es zwingend zu adressieren gilt.

Dank einfacher Tricks können Citrix-Benutzer ihre Rechte erweitern und im schlimmsten Fall mit einigen wenigen Mausclicks die Kontrolle des zugrunde liegenden Hosts erlangen. Die daraus entstehenden Möglichkeiten für einen Angreifer sind beinahe grenzenlos.

Es gilt diesen Risiken mit adäquaten Massnahmen zu begegnen. Bereits beim Design der Umgebung sollte diesen Risiken vorausschauend Rechnung getragen werden und somit bestmöglich zu verhindern.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen setzen namhafte Unternehmen auf die sicherheitstechnische Unterstützung der scip AG.

Zählen auch Sie auf uns:

- Citrix Application Penetration Test
- Citrix Configuration Test
- Citrix Security Audit
- Event Correlation, Handling und Alerting
- Hardening
- Citrix Environment Konzeption
- Konzept Review
- Second Opinion

Herr Chris Widmer freut sich auf Ihre Kontaktaufnahme. Sie erreichen ihn unter der Telefonnummer +41 44 404 13 13 oder via E-Mail an die Adresse chris.widmer@scip.ch

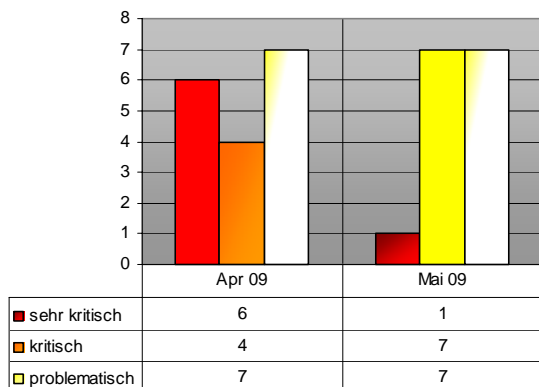
Gerne unterstützen wir Sie bei der erfolgreichen Umsetzung einer sichereren Citrix Infrastruktur.

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:

- 3978 Apple Mac OS X Security Update
- 3975 Apple Safari libxml Pufferüberlauf
- 3974 Powerpoint Sound Data Pufferüberlauf
- 3973 Powerpoint Notes Container Pufferüberlauf
- 3972 Powerpoint BuildList Pufferüberlauf
- 3971 Powerpoint Object Integer Overflow
- 3970 Powerpoint Paragraph Handling Pufferüberlauf
- 3969 Powerpoint unspezifizierte Stack-Overflow Schwachstelle durch spezifische Atome
- 3968 Google Chrome Skia 2D Integer Overflow
- 3964 Symantec WinFax Pro Fax Viewer ActiveX Pufferüberlauf
- 3963 Citrix Web Interface unspezifizierte XSS Schwachstelle
- 3962 Citrix Presentation Server Access Gateway Filters Umgehungsangriff

3.1 Apple Mac OS X Security Update

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 13.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3978>

Mac OS X ist ein kommerzielles Unix-Betriebssystem des Unternehmens Apple und setzt die Produktlinie Mac OS als Betriebssystem der hauseigenen Macintosh-Computer fort. In einem Patchpaket schliesst Apple insgesamt rund 40 Schwachstellen in verschiedenen Betriebssystemkomponenten, die von problematisch bis zu (mehrheitlich) kritisch/sehr kritisch einzustufen sind.

Expertenmeinung:

Apples Politik, nur kumulative Updates herauszugeben, stösst wiederholt auf Kritik: Statt einem grossen Paket möchte man gerne schnelle Fixes von Sicherheitslücken sehen was in Cupertino bislang leider auf taube Ohren zu stossen scheint. Nichtsdestotrotz: Das vorliegende Paket ist für OSX Besitzer absolut zwingend und sollte möglichst zeitnah eingespielt werden.

3.2 Apple Safari libxml Pufferüberlauf

Einstufung: **problematisch**
 Remote: Ja
 Datum: 13.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3975>

Safari ist ein Webbrowser der Firma Apple für das hauseigene Betriebssystem Mac OS X und seit dem 11. Juni 2007 auch für Microsoft Windows, zunächst als Betaversion und seit der Versionsnummer 3.1 als stabile Version, erhältlich ist. Safari gehört zum Lieferumfang von Mac OS X ab der Version 10.3 („Panther“) und ersetzt den vorher mitgelieferten Microsoft Internet Explorer für Mac als Standard-Browser. In Versionen bis 3.2.3 existiert eine Schwachstelle, bei der ein Fehler in libxml zu einem heap-basierten Pufferüberlauf führen kann, was die Ausführung beliebigen Codes erlaubt.

Expertenmeinung:

Auch Apple hat diesen Monat drei Schwachstellen in seinem hauseigenen Browser Safari zu beklagen, die im Rahmen eines kumulativen Patchpaketes gefixt werden. Auch hier lautet die Empfehlung, diese zeitnah zu installieren um eine Exponierung gegenüber

entsprechenden Payloads zu vermeiden.

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3972>

3.3 Powerpoint Sound Data Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 12.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3974>

Microsoft PowerPoint ist ein Computerprogramm, mit dem sich interaktive Folienpräsentationen unter Windows und Mac OS erstellen lassen. In einem Advisory beschreibt Microsoft eine Schwachstelle, bei der Sounddaten nicht korrekt geparkt werden, was zu einem Pufferüberlauf führen kann.

Expertenmeinung:

Sechs Schwachstellen, allesamt kritischer Natur adressiert Microsoft mit diesem kumulativen Patch Release und dürfte damit dem einen oder anderen Administrator etwas Kopferbrechen bereiten. Nichtsdestotrotz sei an dieser Stelle empfohlen, die entsprechenden Updates zeitnah einzuspielen.

3.4 Powerpoint Notes Container Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 12.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3973>

Microsoft PowerPoint ist ein Computerprogramm, mit dem sich interaktive Folienpräsentationen unter Windows und Mac OS erstellen lassen. In einem Advisory beschreibt Microsoft eine Schwachstelle, bei der die Verwendung präpariertes Notes Container zu einem Pufferüberlauf führen kann, der die Ausführung beliebigen Codes begünstigt.

Expertenmeinung:

Sechs Schwachstellen, allesamt kritischer Natur adressiert Microsoft mit diesem kumulativen Patch Release und dürfte damit dem einen oder anderen Administrator etwas Kopferbrechen bereiten. Nichtsdestotrotz sei an dieser Stelle empfohlen, die entsprechenden Updates zeitnah einzuspielen.

3.5 Powerpoint BuildList Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 12.05.2009

Microsoft PowerPoint ist ein Computerprogramm, mit dem sich interaktive Folienpräsentationen unter Windows und Mac OS erstellen lassen. In einem Advisory beschreibt Microsoft eine Schwachstelle, bei der mehrere BuildList Einträge mit ChartBuild Containern zu einem Pufferüberlauf führen können, der die Ausführung beliebigen Codes erlaubt.

Expertenmeinung:

Sechs Schwachstellen, allesamt kritischer Natur adressiert Microsoft mit diesem kumulativen Patch Release und dürfte damit dem einen oder anderen Administrator etwas Kopferbrechen bereiten. Nichtsdestotrotz sei an dieser Stelle empfohlen, die entsprechenden Updates zeitnah einzuspielen.

3.6 Powerpoint Object Integer Overflow

Einstufung: **kritisch**
 Remote: Ja
 Datum: 12.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3971>

Microsoft PowerPoint ist ein Computerprogramm, mit dem sich interaktive Folienpräsentationen unter Windows und Mac OS erstellen lassen. In einem Advisory beschreibt Microsoft eine Schwachstelle, bei der ein Integer Overflow auftritt, wenn die Anzahl spezifischer Elemente überschritten wird, wodurch die Ausführung beliebigen Codes möglich wird.

Expertenmeinung:

Sechs Schwachstellen, allesamt kritischer Natur adressiert Microsoft mit diesem kumulativen Patch Release und dürfte damit dem einen oder anderen Administrator etwas Kopferbrechen bereiten. Nichtsdestotrotz sei an dieser Stelle empfohlen, die entsprechenden Updates zeitnah einzuspielen.

3.7 Powerpoint Paragraph Handling Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 12.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3970>

Microsoft PowerPoint ist ein Computerprogramm, mit dem sich interaktive Folienpräsentationen unter Windows und Mac OS erstellen lassen. In einem Advisory beschreibt Microsoft eine

Schwachstelle, bei der Formatierungsinformation bezüglich einzelner Abschnitte inkorrekt eingelesen und zu einem heap-basierten Pufferüberlauf führen können.

Expertenmeinung:

Sechs Schwachstellen, allesamt kritischer Natur adressiert Microsoft mit diesem kumulativen Patch Release und dürfte damit dem einen oder anderen Administrator etwas Kopferbrechen bereiten. Nichtsdestotrotz sei an dieser Stelle empfohlen, die entsprechenden Updates zeitnah einzuspielen.

3.8 Powerpoint un spezifizierte Stack-Overflow Schwachstelle durch spezifische Atome

Einstufung: **kritisch**
 Remote: Ja
 Datum: 12.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3969>

Microsoft PowerPoint ist ein Computerprogramm, mit dem sich interaktive Folienpräsentationen unter Windows und Mac OS erstellen lassen. In einem Advisory beschreibt Microsoft eine Schwachstelle, bei der gewisse Dateibereiche zur Provokation eines stackbasierten Pufferüberlaufs genutzt werden können.

Expertenmeinung:

Sechs Schwachstellen, allesamt kritischer Natur adressiert Microsoft mit diesem kumulativen Patch Release und dürfte damit dem einen oder anderen Administrator etwas Kopferbrechen bereiten. Nichtsdestotrotz sei an dieser Stelle empfohlen, die entsprechenden Updates zeitnah einzuspielen.

3.9 Google Chrome Skia 2D Integer Overflow

Einstufung: **problematisch**
 Remote: Ja
 Datum: 07.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3968>

Google Chrome ist ein Webbrowser, der von Google Inc. entwickelt wird und seit Dezember 2008 verfügbar ist. Zentrales Konzept ist die Aufteilung des Browsers in optisch und prozesstechnisch getrennte Browser-Tabs. Google Chrome baut auf der Rendering-Engine WebKit auf, die ihrerseits aus dem KDE-Projekt Konqueror hervorging und auch in Apples Browser Safari zum Einsatz kommt. Google beschreibt in einem Advisory zwei Integer

Overflows in der Skia 2D Engine, durch die eine Memory Corruption und möglicherweise die Ausführung beliebigen Codes erreicht werden kann.

Expertenmeinung:

Dass auch Googles Browser nicht vor Sicherheitslücken gefeit ist, zeigt diese Schwachstelle erneut auf. Wie üblich bei Webbrowsern, lautet die Empfehlung hier, möglichst schnell ein Update der entsprechenden Installationen anzustreben.

3.10 Symantec WinFax Pro Fax Viewer ActiveX Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 02.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3964>

Die Symantec Corporation ist ein US-amerikanisches Softwarehaus, welches im Jahr 1982 gegründet wurde. Es ist seit dem 23. Juni 1989 an der NASDAQ börsennotiert. Der Hauptsitz des Unternehmens liegt in Cupertino (Kalifornien/USA), dem geografischen Zentrum des Silicon Valley.. Im Symantec Produkt Winfax Pro findet sich eine Schwachstelle, bei der durch das Symantec.FaxViewerControl.1 ActiveX control (DCCFAXVW.DLL) ein stackbasierter Pufferüberlauf provoziert werden kann, der die Ausführung beliebigen Codes erlaubt.

Expertenmeinung:

Auch wenn der Fax als Telco-Medium etwas ausser Mode geraten wird, ist manch einer von der Anzahl noch in Betrieb befindlicher Faxgeräte und entsprechender Softwarelösungen verblüfft. Der vorliegende Buffer Overflow ist als kritisch einzustufen. Benutzer von WinFax sollten das Killbit für das entsprechende ActiveX Control setzen, um die Exponierung zu vermeiden.

3.11 Citrix Web Interface un spezifizierte XSS Schwachstelle

Einstufung: **problematisch**
 Remote: Ja
 Datum: 01.05.2009
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3963>

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CTXS

scip monthly Security Summary 19.05.2009



gehandelt. Citrix Systems beschäftigt 5.000 Mitarbeiter, die in 35 Ländern Citrix-Lösungen verkaufen. Im Geschäftsjahr 2007 erwirtschaftete Citrix Systems einen Umsatz von 1,4 Milliarden US-Dollar. Im Web Interface des Citrix Access Gateway befindet sich eine unspezifizierte Cross-Site-Scripting Schwachstelle, wie Citrix in einem Advisory meldet. Genauere Details sind bis dato nicht bekannt.

Expertenmeinung:

Wie so oft, sind auch in diesem Fall keine konkreten Informationen zur Lücke veröffentlicht worden, was eine klare Einschätzung erschwert. Es ist davon auszugehen, dass es sich um eine übliche Script Injection Schwachstelle handelt. Es empfiehlt sich daher, den freigegebenen Patch zeitnah einzuspielen.

3.12 Citrix Presentation Server Access Gateway Filters Umgehungsangriff

Einstufung: **problematisch**
Remote: Ja
Datum: 23.04.2009
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3962>

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CTXS gehandelt. Citrix Systems beschäftigt 5.000 Mitarbeiter, die in 35 Ländern Citrix-Lösungen verkaufen. Im Geschäftsjahr 2007 erwirtschaftete Citrix Systems einen Umsatz von 1,4 Milliarden US-Dollar. In einem jüngst veröffentlichten Patch Advisory publizierte Citrix eine Schwachstelle im Presentation Server, bei der durch ein unsauberes Enforcing der Access Policies diverse Sicherheitsmassnahmen umgangen werden können. Dies führt unter Umständen zu einer Kompromittierung des Systems.

Expertenmeinung:

Die vorliegende Schwachstelle ist als problematisch anzusehen, dürfte aber im Regelfall in den meisten Umgebungen nur am Rande zum Tragen kommen. Dennoch sei die Empfehlung gegeben, das freigegebene Patchpaket zeitnah einzuspielen.

4. Statistiken Verletzbarkeiten

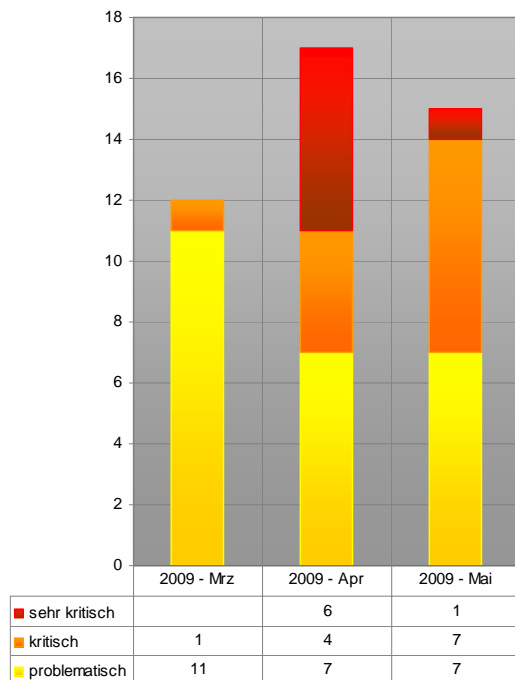
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



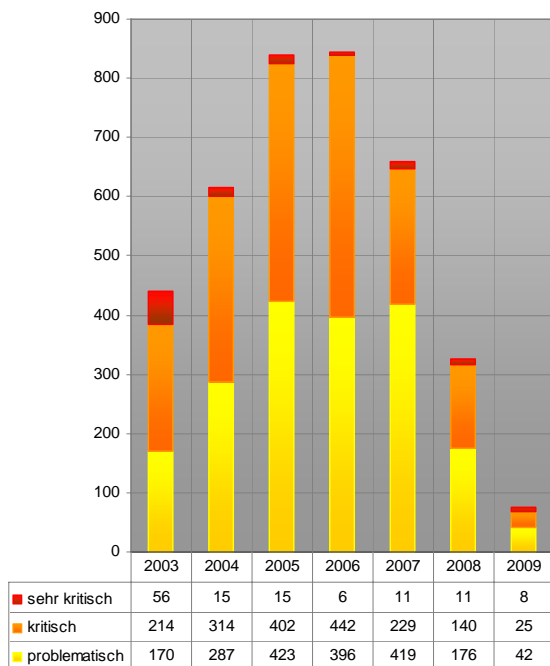
<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

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.

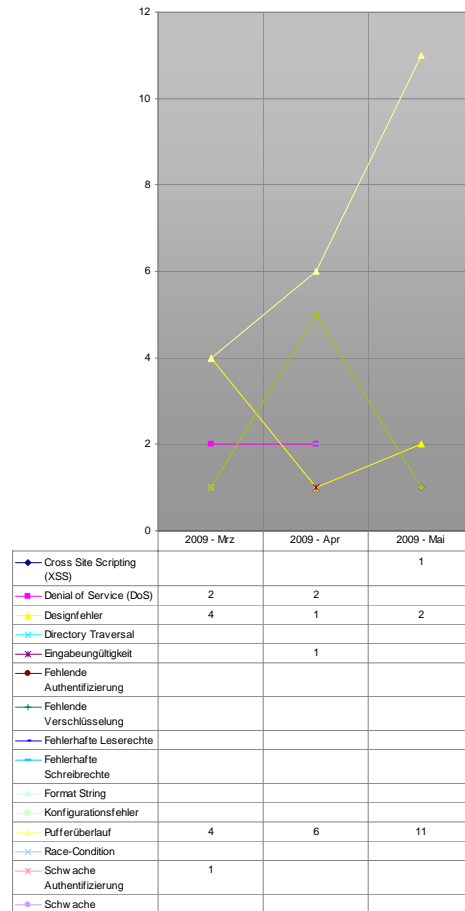
Auswertungsdatum: 19. Mai 2009



Verlauf der Anzahl Schwachstellen pro Jahr

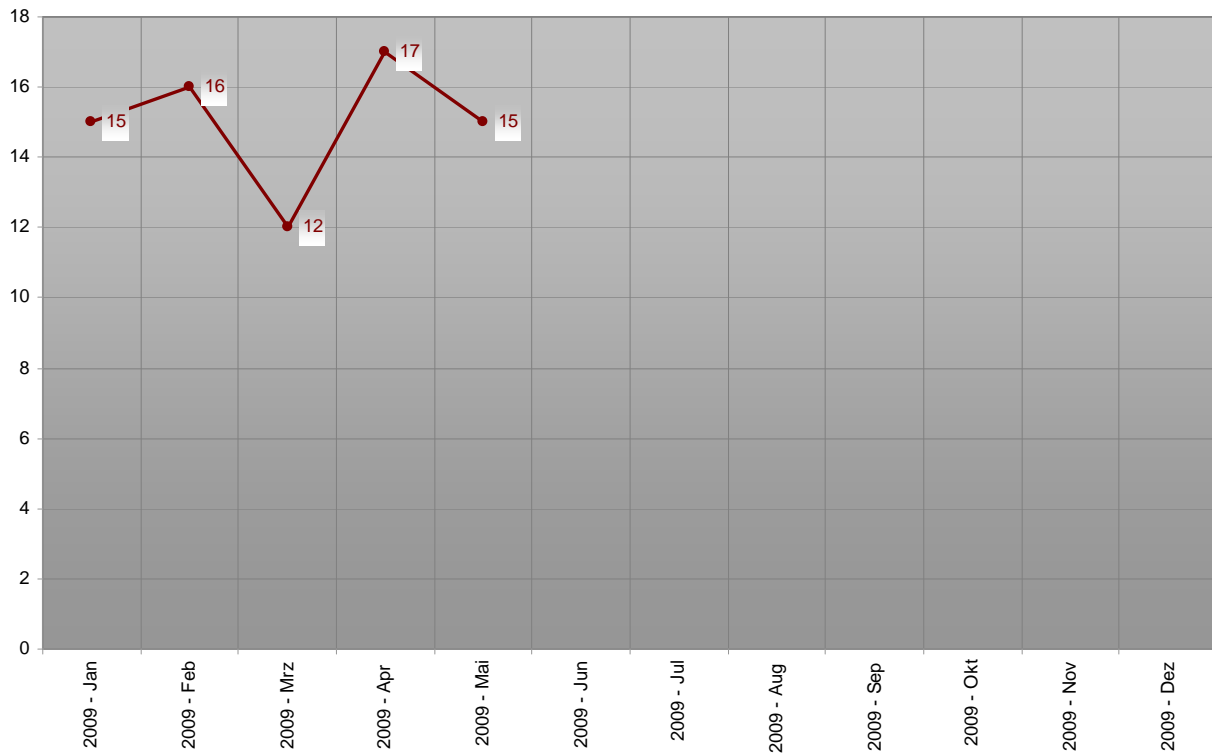


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

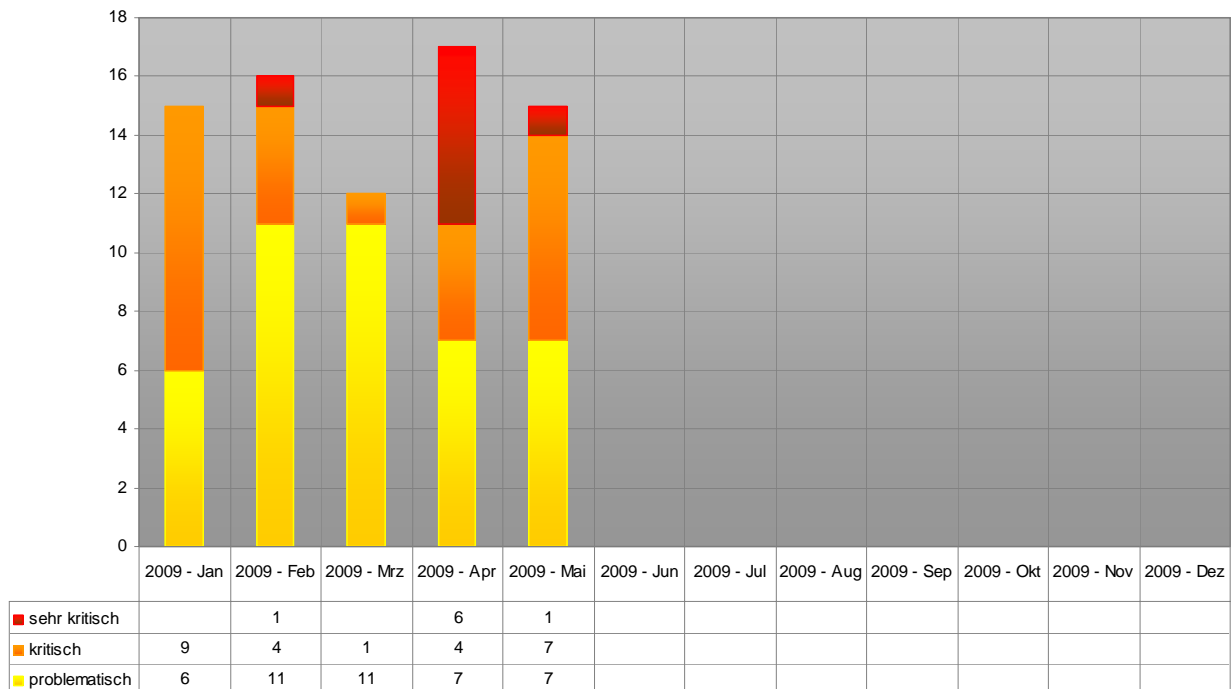


Verlauf der letzten drei Monate Schwachstelle/Kategorie

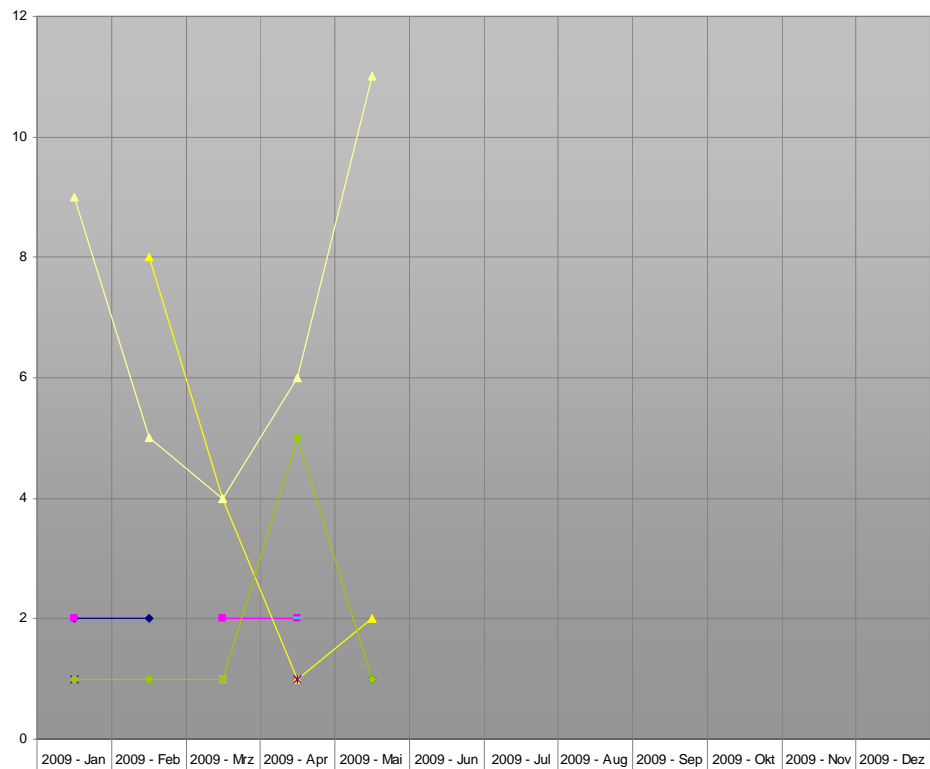
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008-2009



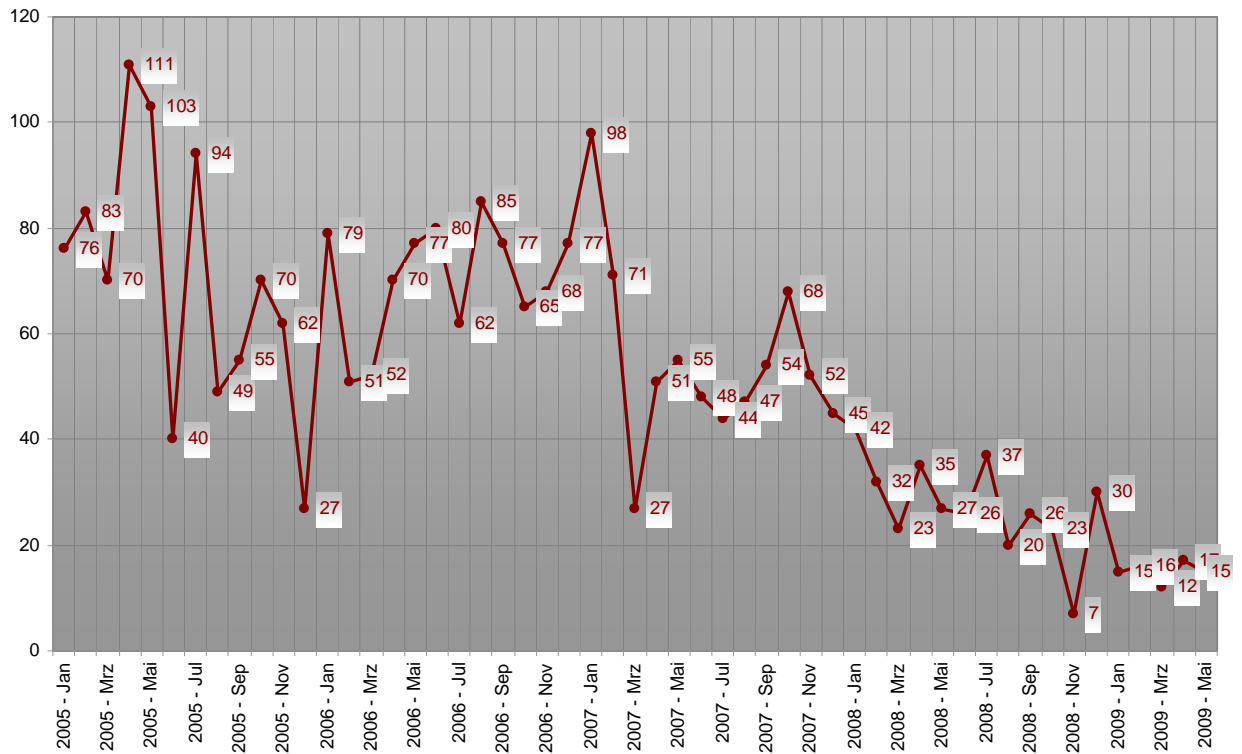
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2009



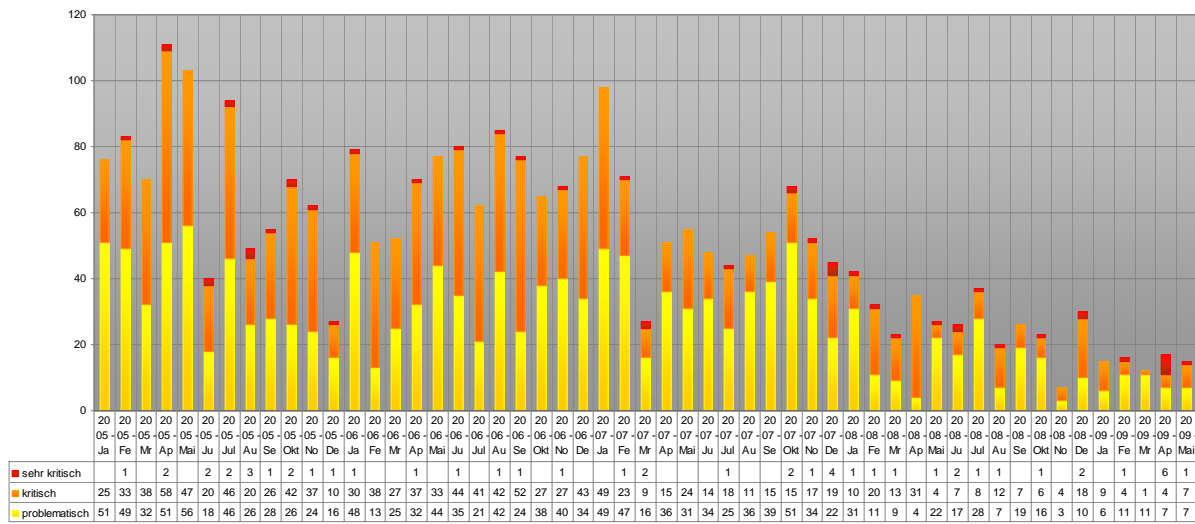
	2009 - Jan	2009 - Feb	2009 - Mrz	2009 - Apr	2009 - Mai	2009 - Jun	2009 - Jul	2009 - Aug	2009 - Sep	2009 - Okt	2009 - Nov	2009 - Dez
◆ Cross Site Scripting (XSS)	2	2			1							
◆ Denial of Service (DoS)	2		2	2								
▲ Designfehler		8	4	1	2							
✕ Directory Traversal												
✖ Eingabeungültigkeit	1			1								
● Fehlende Authentifizierung												
┆ Fehlende Verschlüsselung												
— Fehlerhafte Leserechte												
— Fehlerhafte Schreibrechte												
⋄ Format String												
■ Konfigurationsfehler												
▲ Pufferüberlauf	9	5	4	6	11							
✕ Race-Condition												
✖ Schwache Authentifizierung			1									
◆ Schwache Verschlüsselung												
✕ SQL-Injection												
— Symlink-Schwachstelle												
— Umgehungs-Angriff				2								
◆ Unbekannt	1	1	1	5	1							

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2009

Registrierte Schwachstellen by scip AG

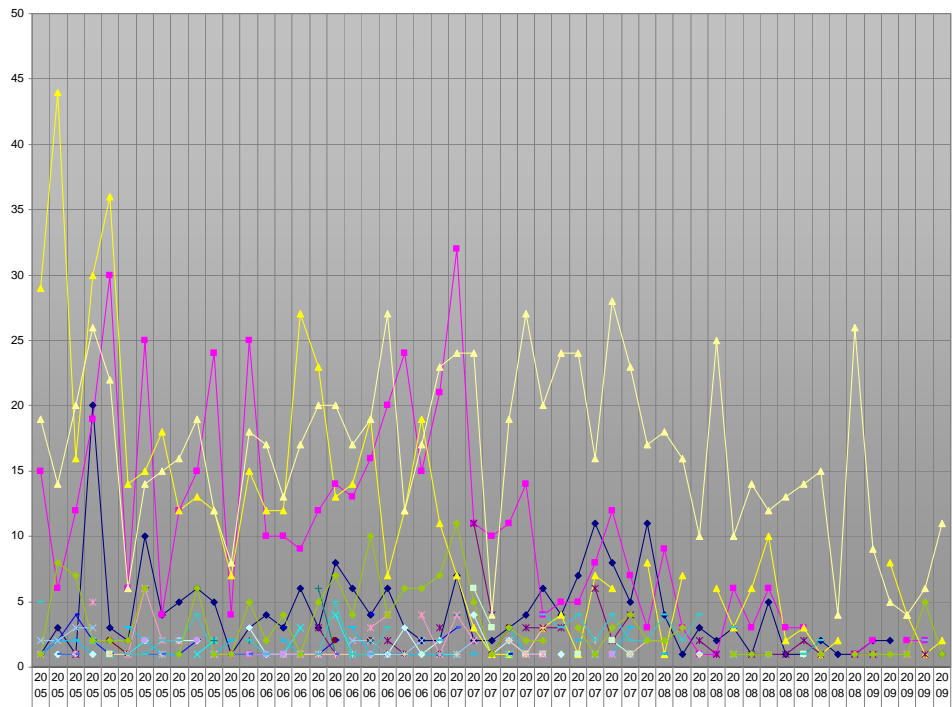


Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005



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	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	6	3	6	3	3	1	2	2	2	2							
◆ 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	1	2									
◆ Directory Traversal			2	1	1	2			1	2			1	1	1	3		4	1					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		1						
◆ Fehlende Authentifizierung			1	2	1							1							2	2	1	1		1	1	3																															
◆ Fehlende Verschlüsselung				2		2	1	2		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																															
◆ 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																											
◆ Konfigurationsfehler					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	10	14	12	13	14	15	4	26	9	5	4	6	11				
◆ Race-Condition	2	2	3	3	1		1			1			1	1	1	1			2	2	1	1	2		1	2	2	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		1		2		2			1	1	1	1					1																																					
◆ SQL-Injection			1	1	1	1	1					1			1	1	1	1					1		1			2	1	3		2	1	2	2	1																					
◆ Symlink-Schwachstelle	1	1	1	2	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				1	2							2				
◆ 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		
9 (english) `s	6 (english)	7 (english)

LÖSUNGSWORT

scip monthly Security Summary 19.05.2009

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 **15.06.2009**. 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. Das **Errata** (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summaries finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)