

Contents

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

1. Editorial

Despotische Demokratie in der virtuellen Welt

Ich kann mich noch sehr gut an einen Penetration Test erinnern, den ich für ein internationales Finanzinstitut durchgeführt habe. Die in Indien eingekaufte Anwendung sollte firmenweit eingesetzt werden und dort die Kommunikation zwischen den Mitarbeitern erlauben. Quasi ein Social Network, wie man es von Xing oder Facebook her kennt, sollte aufgezogen werden. Das Hinzufügen von Kontakten war genauso erwünscht wie der unkomplizierte Austausch von Nachrichten.

Meine Aufgabe bestand nun darin, wenige Wochen vor dem offiziellen Going Live zu überprüfen, ob das System sicher umgesetzt wurde. Schliesslich sollten keine erweiterten Rechte erlangt oder anderweitige Manipulationen umgesetzt werden können. Ein klassischer Penetration Test als nicht-authentisierter und als authentisierter Benutzer wurde angesetzt.

Da geografisch weit voneinander entfernt arbeitende Benutzer an Projekten zusammenarbeiten, werden ebenfalls ein Grossteil der Kurzbesprechungen im virtuellen Raum abgehalten. Dort können dann in Echtzeit Screenshots ausgetauscht und Dokumente bereitgestellt werden. Soetwas ist halt eben

schon nützlich, wenn man als Security Officer in Zürich mal wieder den Entwicklern in Mumbai auf die Füsse treten muss.

Mitunter bietet die Applikation ebenfalls eine Funktion an, im Rahmen einer solchen virtuellen Sitzung eine demokratische Abstimmung durchzuführen: Sodann stellt der Sitzungsleiter oder ein definierter Moderator die Frage in den Raum, wodurch die Sitzungsteilnehmer durch das Klick auf einen Button ihre Stimme mit Ja/Nein abgeben können. Sofort nach Durchführung dieser Abstimmung werden die Stimmen ausgezählt und das Resultat präsentiert. Selbst Entscheidungen grösserer Tragweite sollen auf derartige Weise unkompliziert verabschiedet werden.

Im Rahmen meiner Prüfung habe ich einen Fehler bei der Übermittlung der Stimmenabgabe gefunden. Der Client schickt nicht nur 1 (Ja) oder 0 (Nein) als eigentliche Stimme an den Server. Stattdessen wird zusätzlich die Client-ID selbst bestimmt und mitgeschickt. Hierbei handelt es sich um die Benutzer-ID des Anwenders, der seine Stimme abgibt. Da nun die Möglichkeit besteht, dass ein Client die ID eines anderen Clients vortäuschen kann, kann er im Rahmen der Abstimmung die Stimmen der anderen Benutzer vergeben. Gebe ich anstelle meiner ID 42 die ID 23 mit, kann ich für den Benutzer 23 abstimmen.

Die Folge davon ist, dass ein manipulierter Client noch vor der legitimen Stimmabgabe der echten Clients seine manipulativen Stimmeeinlagen durchsetzen kann. Die als erstes beim Server angekommene Stimme wird gezählt. Der vorgetäuschte Client kommt von diesem Prozess nichts mit, denn bei ihm wird die abgegebene Stimme angezeigt, so wie er sie selbst vergeben hat. Schon doof, wenn Server und Client mit unterschiedlichen Daten arbeiten, oder? Der Client verzichtet darauf, die effektiv auf dem Server ausgezählten Stimmen mit den eigenen Daten im lokalen Cache zu vergleichen bzw. synchronisieren.

Es stellt sich die grosse Frage, warum gerade in diesem Punkt (und einigen anderen) der Client dafür verantwortlich ist, sich selber während einer etablierten Session nocheinmal

auszuweisen. Dies ist ein typisches Anfängerproblem bzw. eine bekannte Nachlässigkeit von Entwicklern, dass sie halt eben gewisse Teile des Session-Handlings an den Client auslagern. Grundsätzlich muss man sich aber immer bewusst sein, dass man den Client nie gänzlich unter Kontrolle halten kann. Es wird immer Leute geben, die Zeit und Aufwand nicht scheuen, um clientseitig einen Vorteil erarbeiten zu können. In diesem Fall besteht der Vorteil darin, vermeintlich demokratische Entscheidungen manipulieren zu können. Welcher Despot träumt nicht von dieser Möglichkeit?

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 1. Juni 2009

2. scip AG Informationen

2.1 Security Coaching

Das Ziel unserer Dienstleistung Security Coaching ist die direkte Beratung und unmittelbares Coaching. Dies mit dem Hintergrund zur Diskussion, Verhinderung und Einschränkung der Etablierung von Designschwächen und akuten Schwachstellen im Projekt, in den Prozessen sowie mit der ganzheitlichen Sichtweise basierend auf den Firmenbedürfnissen.

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

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

In erster Linie soll in beratender Weise eine direkte Hilfestellung mit konkreten Empfehlungen und Lösungen bereitgestellt werden.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen haben wir als scip AG bereits eine Vielzahl von Security Coaching Projekte durchgeführt.

Zählen auch Sie auf uns!

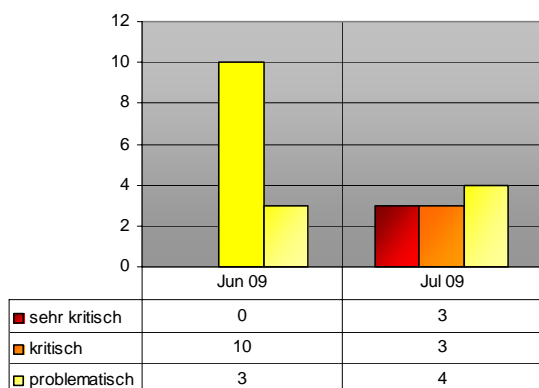
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch.

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:

- 4002 Oracle Produkte verschiedene Schwachstellen
- 4001 Microsoft DirectShow Streaming Video ActiveX Control
- 4000 Microsoft Office Web Components Codeausführung
- 3998 Windows Embedded OpenType Font Engine Integer Overflow
- 3997 Windows Embedded OpenType Font Engine Integer Truncation
- 3994 VLC Media Player SMB Input Module Pufferüberlauf
- 3993 Google Chrome JS Regexp Pufferüberlauf
- 3992 Google Chrome HTTP Response Pufferüberlauf
- 3991 Foxit Reader JPEG2000/JBIG Decoder Pufferüberlauf

3.1 Oracle Produkte verschiedene Schwachstellen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 15.07.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4002>

Oracle Corporation ist der weltweit drittgrößte Softwarehersteller[1] mit Hauptsitz in Redwood Shores (Silicon Valley, Kalifornien). Bekanntestes und erfolgreichstes Produkt des Unternehmens ist das Datenbankmanagementsystem Oracle Database, welches üblicherweise mit dem Namen Oracle in Verbindung gebracht wird. In einem kumulativen Softwareupdate fixt Oracle eine Vielzahl von Schwachstellen, die seit längerer Zeit offen waren und teilweise kritische Sicherheitslücken darstellten.

Expertenmeinung:

Oracles Praxis, Schwachstellen nur in grossen Patchpaketen zu schliessen, hat schon so oft für rote Köpfe gesucht. Auch in diesem Fall wird das vorliegende Patchpaket sicherlich nur in begrenztem Rahmen mit offenen Armen empfangen werden. Dennoch sei Oracle Administratoren ans Herz gelegt, die entsprechenden Patches zeitnah zur Einspielung zu bringen.

3.2 Microsoft DirectShow Streaming Video ActiveX Control

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 14.07.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4001>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. In einer ActiveX Komponente, die Nutzung der DLL msvidctl.dll macht, besteht eine Schwachstelle die zur Ausführung beliebigen Codes auf dem Zielsystem genutzt werden kann, wenn auf dem Zielsystem z.B. eine präparierte HTML Seite geladen wird.

Expertenmeinung:

Diese Schwachstelle wird momentan aktiv ausgenutzt und wurde als 0-Day gemeldet. Längst sind entsprechende Exploits öffentlich verfügbar und werden flächendeckend eingesetzt. Betroffene Administratoren sollten zeitnah darum bemüht sein, das Killbit der entsprechenden Komponenten zu setzen, um eine Kompromittierung zu verhindern.

3.3 Microsoft Office Web Components Codeausführung

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 13.07.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4000>

Microsoft Office ist das Office-Paket des US-amerikanischen Unternehmens Microsoft für die Betriebssysteme Microsoft Windows und Mac OS. Für unterschiedliche Aufgabenstellungen werden verschiedene Suiten angeboten, die sich in den enthaltenen Komponenten, dem Preis und der Lizenzierung unterscheiden. In verschiedenen Versionen von Microsoft Office (2003, XP) wird ein verwundbares Paket, die sogenannten Web Components mitgeliefert. Dieses Set von ActiveX Komponenten kann dazu genutzt werden, Office Dokumente und -Objekte innerhalb des Internet Explorers zu verwenden. Durch einen Pufferüberlauf bei der Einbindung dieser Objekte, kann beliebiger Code zur Ausführung gebracht werden.

Expertenmeinung:

Diese Schwachstelle wird momentan aktiv ausgenutzt und wurde als 0-Day gemeldet. Längst sind entsprechende Exploits öffentlich verfügbar und werden flächendeckend eingesetzt. Betroffene Administratoren sollten zeitnah darum bemüht sein, das Killbit der entsprechenden Komponenten zu setzen, um eine Kompromittierung zu verhindern.

3.4 Windows Embedded OpenType Font Engine Integer Overflow

Einstufung: **kritisch**
 Remote: Ja
 Datum: 14.07.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3998>

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

Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. In der OpenType Font Engine existiert ein Integer Overflow Problem, das von einem Angreifer zum Zwecke eines Pufferüberlaufs ausgenutzt werden kann.

Expertenmeinung:

Die OpenType Font Engine ist eine Standardkomponente von Windows und somit hoch verbreitet, was die Schwachstelle kritisch macht. Der bereitgestellte Patch sollte zeitnah eingespielt werden, um eine Kompromittierung durch Dritte zu vermeiden.

3.5 Windows Embedded OpenType Font Engine Integer Truncation

Einstufung: **kritisch**
 Remote: Ja
 Datum: 14.07.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3997>

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS), inzwischen wurde dieser Entwicklungszweig zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. In der OpenType Font Engine existiert ein Integer Truncation Problem, das von einem Angreifer zum Zwecke eines Pufferüberlaufs ausgenutzt werden kann.

Expertenmeinung:

Die OpenType Font Engine ist eine Standardkomponente von Windows und somit hoch verbreitet, was die Schwachstelle kritisch macht. Der bereitgestellte Patch sollte zeitnah eingespielt werden, um eine Kompromittierung durch Dritte zu vermeiden.

3.6 VLC Media Player SMB Input Module Pufferüberlauf

Einstufung: **problematisch**
 Remote: Ja
 Datum: 26.07.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3994>

Der VLC media player (anfänglich VideoLAN Client) ist ein portabler, freier Mediaplayer sowohl für diverse Audio-, Videocodecs und Dateiformate als auch DVDs, Video-CDs und



unterstützt unterschiedliche Streaming-Protokolle. Er kann auch als Server zum Streaming in Uni- oder Multicast in IPv4 und IPv6 oder als Transcoder für die unterstützten Video und Audio-Formate verwendet werden. In aktuellen Versionen der Windowsversion von VLC wurde ein stackbasierter Pufferüberlauf identifiziert, der beim Aufruf der Win32AddConnection() in modules/access/smb.c ausgelöst werden kann. Durch das Öffnen einer manipulierten Playlist kann das Zielsystem kompromittiert werden.

Expertenmeinung:

Die vorliegende Schwachstelle betrifft ausschliesslich die Windows Version von VLC, ist hier aber als problematisch zu werten. Anwender der betroffenen Software sollten zeitnah ein Update einspielen.

3.7 Google Chrome JS Regexp Pufferüberlauf

Einstufung: **sehr kritisch**

Remote: Ja

Datum: 17.07.2009

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3993>

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. Das Chrome Security Team gab unlängst eine Schwachstelle bekannt, die durch einen Fehler im Handling von regulären Ausdrücken in Javascript auftrat. Durch die Schwachstelle konnte ein Pufferüberlauf verursacht werden, was zur Kompromittierung des Systems führte.

Expertenmeinung:

Auch Googles Hausbrowser ist vor derartigen Schwächen, wie sie auch schon in anderen Produkten angetroffen werden konnten, nicht gefeit. Der Hersteller empfiehlt das herausgegeben Update zeitnah zu installieren.

3.8 Google Chrome HTTP Response Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 23.06.2009

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3992>

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. Das Chrome Security Team gab unlängst eine Schwachstelle bekannt, die durch einen Fehler im Handling von un spezifizierten HTTP Antworten auftrat. Durch die Schwachstelle konnte ein Pufferüberlauf verursacht werden, was zur Kompromittierung des Systems führte.

Expertenmeinung:

Auch Googles Hausbrowser ist vor derartigen Schwächen, wie sie auch schon in anderen Produkten angetroffen werden konnten, nicht gefeit. Der Hersteller empfiehlt das herausgegeben Update zeitnah zu installieren.

3.9 Foxit Reader JPEG2000/JBIG Decoder Pufferüberlauf

Einstufung: **problematisch**

Remote: Ja

Datum: 22.06.2009

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3991>

FoxIT Reader ist ein mehrsprachiger PDF Reader, der in einer freien und einer kommerziellen Version von FoxIT Software angeboten wird. Will Dormann identifizierte einen Pufferüberlauf in aktuellen Versionen, mittels dem sich eine Kompromittierung des Zielsystems anstreben lässt.

Expertenmeinung:

FoxIT wurde im Anbetracht der sich häufenden Schwachstellen in Adobe Reader oftmals als Alternative empfohlen - wie sich nun herausstellt, nicht ganz zu recht. Anwender und Administratoren, die die Software einsetzen, sollten sich zeitnah nach einer Alternative umsehen oder auf die neuste Version updaten.

4. Statistiken Verletzbarkeiten

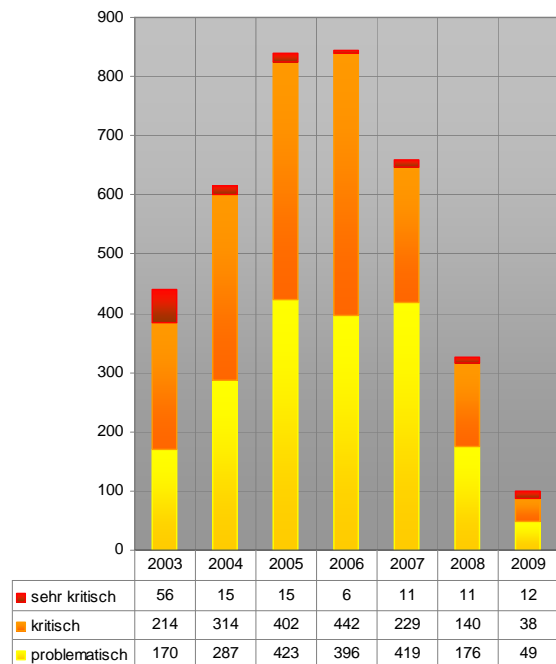
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



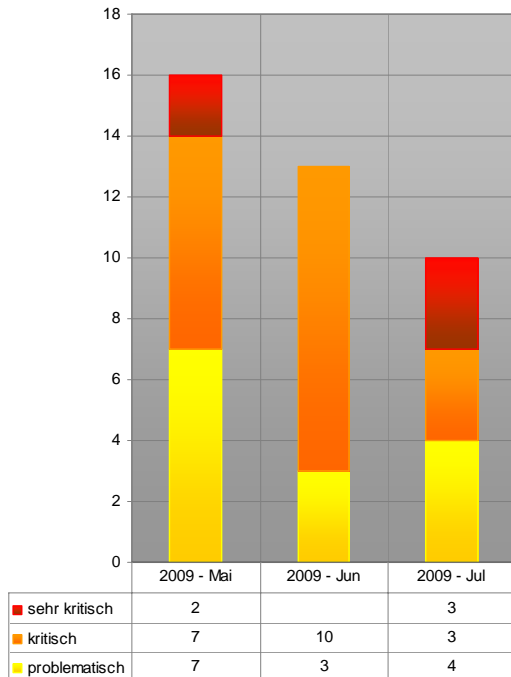
<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

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.

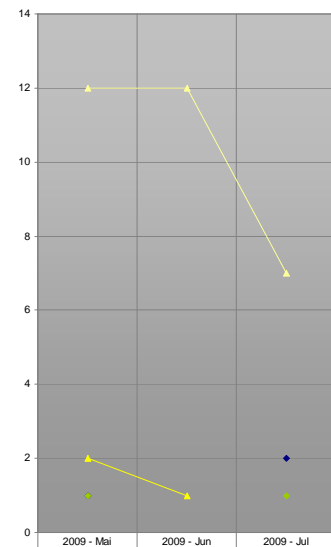
Auswertungsdatum: 17. Juli 2009



Verlauf der Anzahl Schwachstellen pro Jahr



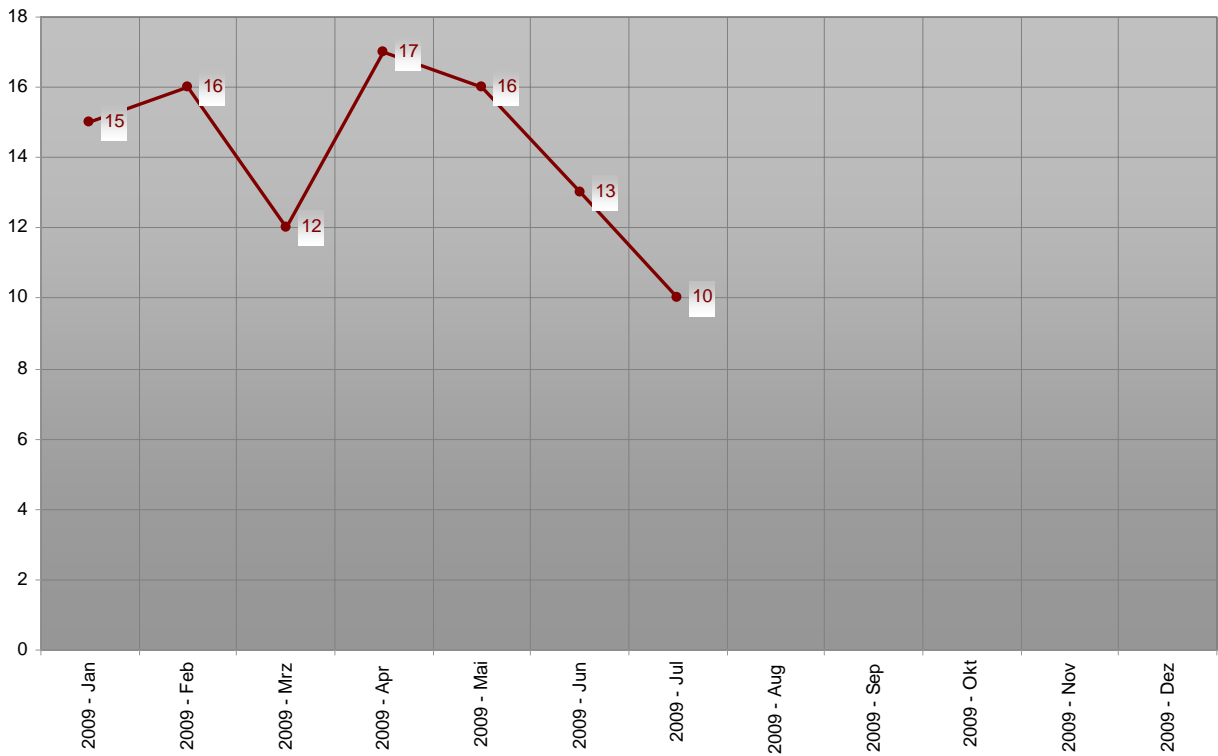
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



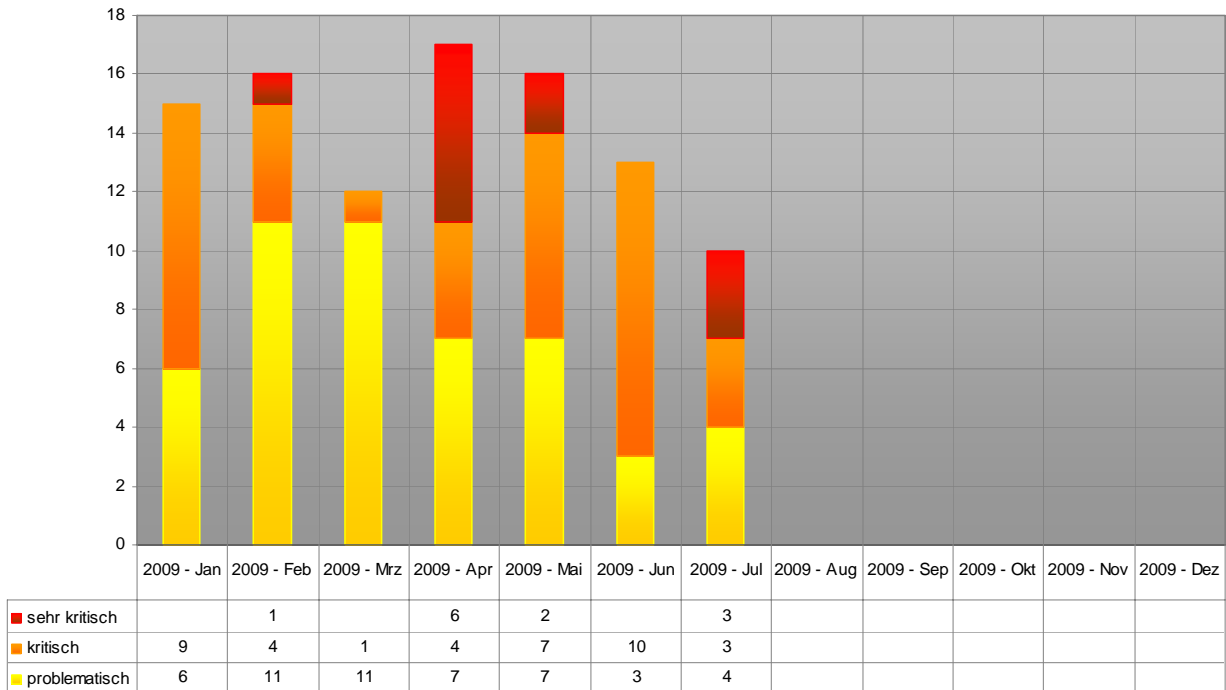
	2009 - Mai	2009 - Jun	2009 - Jul
Cross Site Scripting (XSS)	1		2
Denial of Service (DoS)			
Designfehler	2	1	
Directory Traversal			
Eingabeungültigkeit			
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Format String			
Konfigurationsfehler			
Pufferüberlauf	12	12	7
Race-Condition			
Schwache Authentifizierung			
Schwache			

Verlauf der letzten drei Monate Schwachstelle/Kategorie

Registrierte Schwachstellen by scip AG



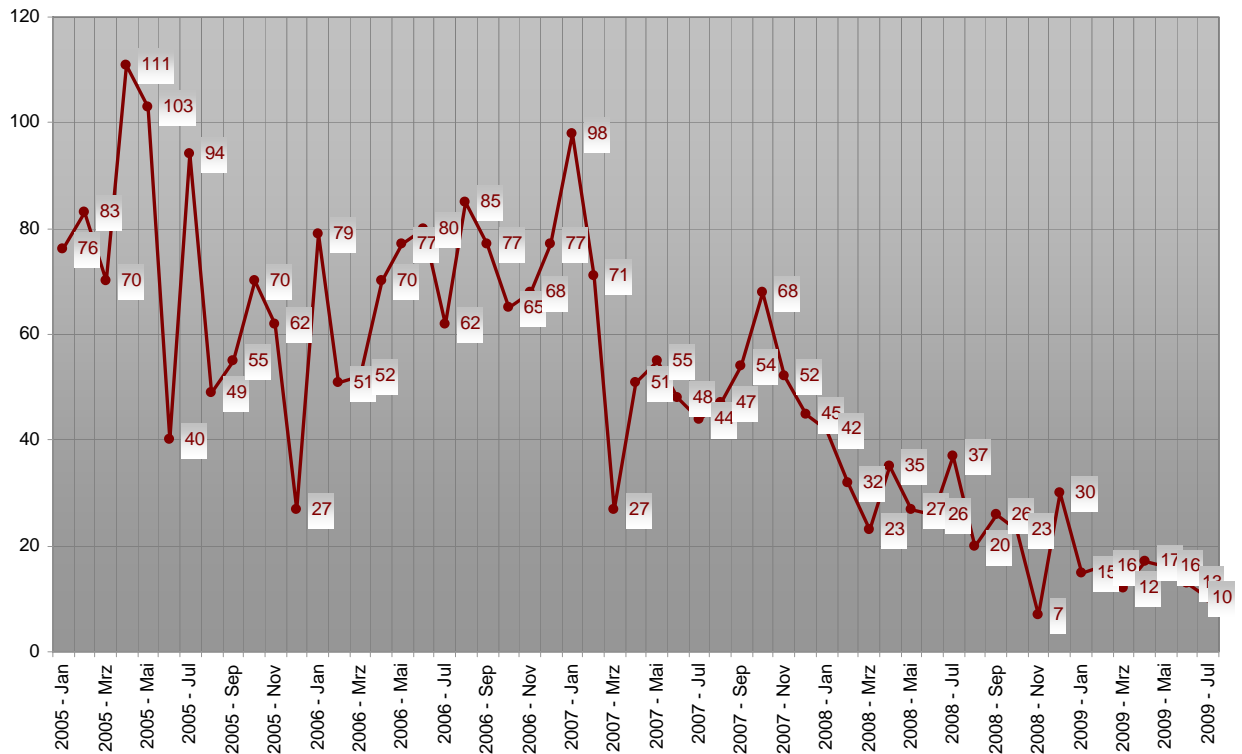
Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008-2009



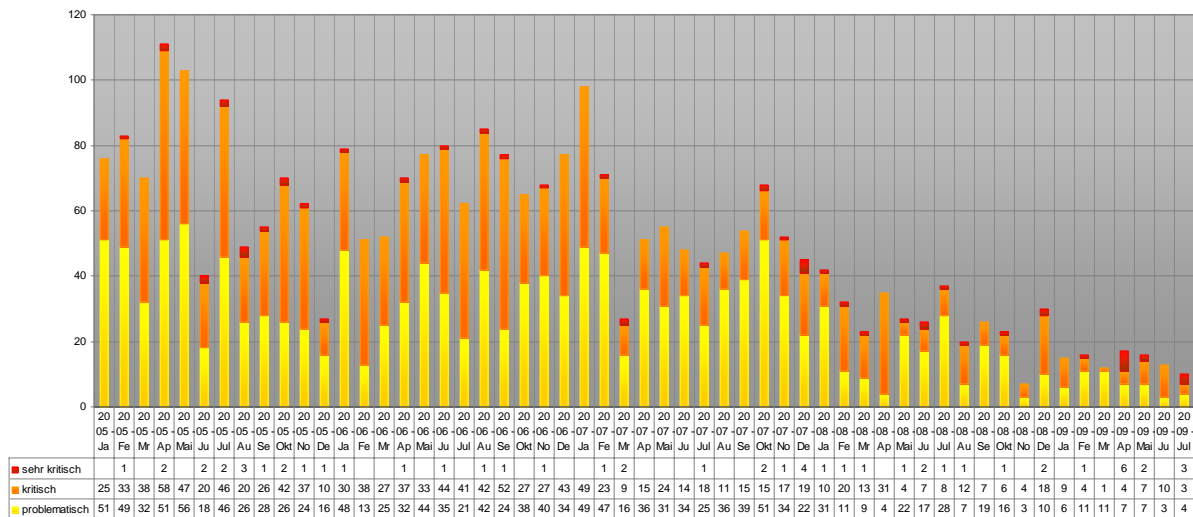
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2009



Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005



5. Bilderrätsel



GESUCHTE BEGRIFFE

9 (english)	14 (english)	11 (english)

LÖSUNGSWORT

Wettbewerb

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

Einsendeschluss ist der **15.08.2009**. 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 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. Das **Errata** (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summaries finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)