)SCIP(

scip ag

Contents

1. Editorial

Potentielle, existente, ausnutzbare oder ausgenutzte Schwachstellen

Ich arbeite nun schon über einem Jahrzehnt im Bereich der Computersicherheit, habe schon hunderte von Audit-Projekten durchgeführt, zehntausende von Hosts angegriffen und hunderttausende von Ports gescannt. Alle diese Projekte waren anders. Und doch hatten viele von ihnen etwas gemein: Der Kunde wusste oftmals nicht, was er genau möchte. Sehr generisch und dennoch knapp formuliert definiert sich das Ziel einer Sicherheitsüberprüfung meistens wie folgt: "Es sollen Schwachstellen aufgedeckt werden." Doch Schwachstellen sind nicht gleich Schwachstellen und Aufdecken ist nicht gleich Aufdecken.

So gilt es beispielsweise zu unterscheiden, ob man nun potentielle, existente, ausnutzbare oder ausgenutzte Schwachstellen ausmachen möchte. Jenachdem ist hierzu ein gänzlich unterschiedliches Vorgehen erforderlich. Bei potentiellen Schwachstellen wird versucht möglichst breitflächig zu agieren, um die gesamte Angriffsfläche ermitteln zu können. Beim Ausmachen existenter Schwachstellen muss sich hingegen eher auf Angriffspunkte fokussiert werden, um durch das explizite Ausnutzen dieser deren Vorhandensein zu beweisen.

Obschon diese Aspekte alle das gleiche höherwertige Ziel verfolgen, ist also ein gänzlich unterschiedliches Vorgehen und damit auch ein ganz anderes Toolset erforderlich. Breitflächige Analysen erfordern Tools und Skripte, die immerwiederkehrende Auswertungen automatisieren. Nmap (inkl. NSE-Engine) oder Nessus sind typische Hilfsmittel hierzu. Gezielte Angriffe erfordern hingegen Frameworks, die das Generieren und Replizieren von Zugriffen und Payloads erleichtern. Hier kommen Mechanismen wie die Web Developer Toolbar für Firefox oder das MetaSploit Framework (MSF) zum Tragen. Die eine Arbeit kann mit der Herangehensweise und den Werkzeugen der anderen nicht ebenfalls effizient oder gar nicht ausgeführt werden.

Da so mancher Kunde überhaupt nicht weiss, was er von einer Sicherheitsüberprüfung will, kann er von sich aus auch gar nicht nachvollziehen, welche Herangehensweise und welche Mittel zum Erreichen der Ziele - die man versucht hat mit ihm zu definieren - erforderlich sind. Unverständnis und Diskussionen können sodann plötzlich mitten in einem Projekt vorkommen.

Verkaufen wir beispielsweise einen netzwerkbasierten Security Scan, so erfordert dieser möglichst direkten Zugriff auf die Zielsysteme. Bei lokalen Scans vor Ort ist hierzu mindestens ein RJ45-Anschluss und eine legitime Adressierung in der gleichen Zone des Zielsystems erforderlich. Anpassungen am DHCP-Server oder in den VLAN-Konfigurationen können hierzu erforderlich sein. (Zwar lassen sich solche Scans theoretisch auch über verschiedene Zonen und Firewall-Systeme hinweg durchführen. Die akademische Genauigkeit der Analyse leidet jedoch unter den Bedürfnissen eines Real-World Angriffsszenarios.)

Im Rahmen eines solchen Projekts wurde uns leider am Tag des angesetzten Scans mitgeteilt, dass wir keinen Zugriff - so wie gewünscht und frühzeitig definiert wurde - erhalten würden. "Sehr schade", entgegnete ich, "denn so müssen wir halt nun auf die Umsetzung dieses Testmoduls verzichten." Dem Kunden war dies natürlich nicht recht, denn die Qualitätssicherung des Unternehmens sieht vor, dass vor einer Freigabe eines Dienstes dieser eben einer

Sicherheitsüberprüfung durch eine externe Firma unterzogen werden muss.

Der Projektleiter auf der Kundenseite fragte sodann nach, ob wir denn nicht mit einem Direktzugriff auf die Systeme per SSH entsprechende Auswertungen durchführen können. "Selbstverständlich können wir das", war meine Antwort. "Doch eine derartige Betrachtung kann", führte ich weiter aus, "einen Netzwerkscan nicht gänzlich ersetzen." Meine Aussage generierte ausschliesslich Unverständnis.

Ich habe dem Kunden versucht zu erklären, dass ein Arzt zwar in so manchem Fall die gleiche Krankheit erkennen kann, egal ob er nun den Patienten einer Röntgenuntersuchung unterzieht oder ob er eine Blutprobe nimmt. Es gibt aber viele Krankheitsbilder, die lassen sich nur mit erheblichem Aufwand oder gar nicht zuverlässig mit nur einer der beiden Methoden ausmachen. Genauso verhält es sich bei Netzwerkscans und lokalen Analysen. Im besten Fall macht man natürlich beides bzw. alle möglichen Tests.

Das Problem hierbei ist, dass dem Kunden nur mit erheblichem technischen Verständnis bewusst wäre, welche Vor- und Nachteile die einzelnen Testvarianten mit sich führen würden. Jenachdem setzt er sich nämlich gewissen Risiken aus, wenn er auf bestimmte Tests verzichtet. Es ist sodann Aufgabe des Consultants, ihm die unterschiedlichen Aspekte zu erläutern. Eine Aufgabe, die manchmal nicht besonders einfach ist.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 17. Mai 2010

2. scip AG Informationen

2.1 Backdoor Test

Das Ziel unserer Dienstleistung Backdoor Test ist die erfolgreiche Kompromittierung der Zielumgebung durch die Infektion eines eigens angefertigten Trojanischen Pferds (Backdoor) zur Bestimmung effektiv ausnutzbarer Schlupflöcher im bestehenden Sicherheitsdispositiv.

- Vorbereitung: Die Zielumgebung wird ausgewertet, um ein individuelles Angriffsszenario entwickelt.
- Entwicklung: Ein Trojanisches Pferd wird für den Kunden programmiert. Wir bauen dabei auf unsere eigenen Code Libraries und Exploiting Payloads. SAP, iPhone, Web 2.0/Ajax, Windows Mobile, Word, Excel, PowerPoint, PDF, Outlook, Lotus Notes etc.
- Infektion: Die Zielumgebung oder ein definiertes Zielsystem wird mit dem Trojanischen Pferd infiziert (z.B. Social Engineering, Drive-By Infection, Exploiting einer Dokumentenschwachstelle).
- Fernsteuerung: Nach erfolgreicher Infektion wird die Fernsteuerung durchgesetzt, um die Machbarkeit und Möglichkeiten zu demonstrieren.

Solcherlei Backdoor Inside/Out Tests sind sehr individuell. Die Vorbereitungen (Entwicklung der Hintertür) sowie die Durchführung des Angriffs (Infektion und Fernsteuerung) werden detailliert dokumentiert. Die ausgenutzten Schwächen der Zielumgebung (z.B. Firewall-Tunneling, Antivirus Evasion, etc.) werden ausführlich besprochen.

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

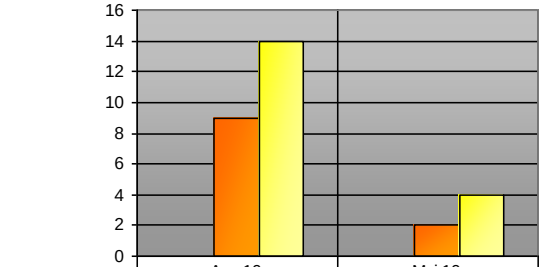
Zählen auch Sie auf uns!
http://www.scip.ch/?firma.referenzenalle

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/?vuldb einsehbar.

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



	Apr 10	Mai 10
sehr kritisch	0	0
kritisch	9	2
problematisch	14	4

Contents:

3.1 Adobe Photoshop CS4 TIFF Verarbeitungsschwachstelle

Risiko: kritisch
Remote: Ja
Datum: 03.05.2010
scip DB: http://www.scip.ch/?vuldb.4131

Adobe Photoshop ist ein kommerzielles Bildbearbeitungsprogramm des US-amerikanischen Softwarehauses Adobe Systems. Im Bereich der professionellen Bildbearbeitung (Druckvorstufe) ist das Programm Marktführer. Photoshop ist Teil der Adobe Creative Suite, einer Sammlung von Grafik- und Designprogrammen und wie die meisten anderen Adobe-Anwendungen für Mac OS X und Microsoft Windows verfügbar. Der Researcher Tavis Ormandy beschreibt in einem Advisory eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der Applikation. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:
Auch wenn der Angriffsvektor etwas umständlich ist, ist die vorliegende Schwachstelle aufgrund der hohen Popularität von Photoshop als durchaus kritisch zu betrachten. Der freigegebene Patch von Adobe sollte zeitnah eingespielt werden, um eine weitere Exponierung zu vermeiden.

3.2 Apple Safari Codeausführung

Risiko: kritisch
Remote: Ja
Datum: 07.05.2010
scip DB: http://www.scip.ch/?vuldb.4130

Safari ist ein Webbrowser des Unternehmens 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. Safari gehört zum Lieferumfang von Mac OS X ab der Version 10.3 ("Panther") und ersetzte den vorher mitgelieferten Microsoft Internet Explorer für Mac als Standard-Browser. Der Researcher Krystian Kloskowski beschreibt in einem Advisory eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der Applikation. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

Expertenmeinung:
Auch Safari ist vor neuen Angriffen nicht gefeit. Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah durch ein Softwareupdate adressiert werden.

3.3 vBulletin BB Code Script Insertion

Risiko: problematisch
Remote: Ja
Datum: 07.05.2010
scip DB: http://www.scip.ch/?vuldb.4129

vBulletin ist eine in der Skriptsprache PHP geschriebene proprietäre Softwarelösung für Webforen und soziale Netzwerke. Zur Speicherung von Inhalten wird die Datenbank MySQL genutzt. Der Researcher MaXe identifizierte unlängst eine Schwachstelle (Cross Site Scripting (XSS)) in aktuellen Versionen der vorliegenden Applikation. Die vorliegende Schwachstelle erlaubt es, aufgrund eines Fehlers in der Eingabevalidierung des Produktes, beliebigen Scriptcode zu injizieren und damit im Kontext des Browsers zur Ausf• hrung zu bringen.

Expertenmeinung:
Script Injection Schwachstellen sind grundsätzlich sehr einfache, aber ärgerliche Schwachstellen mit potentiell hoher Schadenswirkung in Kombination mit anderen Angriffsvektoren. Betroffene Installationen sollten daher zeitnah auf eine aktualisierte Version migriert werden. Alternativ kann eigenständig ein Fix implementiert werden, bis ein offizieller Patch zur Verfügung steht.

3.4 Wireshark DOCSIS Dissector Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 06.05.2010
scip DB: http://www.scip.ch/?vuldb.4128

Wireshark (engl. "wire": Draht, Kabel; "shark": Hai; alte Bezeichnung: Ethereal) ist ein freies Programm zur Analyse von Netzwerk-Kommunikationsverbindungen. Die Entwickler des popul„ren Netzwerk-Analysetools Wireshark veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Denial of Service (DoS)) in verschiedenen Versionen des Produktes beschreibt. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und - unter Umständen - beliebigen Code zur Ausführung bringen.

Expertenmeinung:
Die vorliegende Schwachstelle reiht sich einigermassen nahtlos in eine Reihe von Dissektoren-Schwachstellen ein. Zwar kann hierbei keine Code Execution erreicht werden, jedoch ist auch der angestrebte Denial of Service eher ärgerlich. Daher sollten Benutzer zeitnah eine aktualisierte Version einspielen, in der der geschilderte Bug behoben wurde.

3.5 Pidgin MSN SLP Message Custom Emoticon Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 13.05.2010
scip DB: http://www.scip.ch/?vuldb.4127

Pidgin (früher Gaim, nicht zu verwechseln mit Gajim) ist ein freier Multi-Protokoll-Client, der von Mark Spencer ursprünglich für unixähnliche Systeme (Linux, BSD) geschrieben wurde, inzwischen aber auch auf Microsoft Windows lauffähig ist und mit Plug-ins stark erweitert werden kann. Der Researcher Pierre Noguès der Firma Meta Security identifizierte unlängst eine Schwachstelle (Denial of Service (DoS)) in aktuellen Versionen der vorliegenden Applikation. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und - unter Umständen - beliebigen Code zur Ausführung bringen.

Expertenmeinung:
Pidgin ist als IM Client populär und für verschiedene Plattformen lauffähig. Betroffene Benutzer sollten aufgrund der Popularität der Software zeitnah dazu übergehen, eine aktualisierte Version zu verwenden.

3.6 Outlook Express / Windows Mail STAT Response Integer Overflow

Risiko: problematisch
Remote: Ja
Datum: 11.05.2010
scip DB: http://www.scip.ch/?vuldb.4126

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 zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Der Researcher Francis Provencher der Firma Protek

Research Labs beschreibt in einem Advisory eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der Applikation. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:
Die vorliegende Schwachstelle ist sicherlich als problematisch zu betrachten, bedingt aber dass das Opfer sich dazu bewegen lässt, zu einem entsprechend manipulierten POP3 Server zu verbinden. Das Anriffsszenario benötigt daher zusätzlichen Massnahmen (z.B. Social Engineering), weshalb von einer kritischen Einstufung abgesehen wird. Trotzdem sollte die Schwachstelle zeitnah durch das Einspielen entsprechender Patches behoben werden, um eine unnötige Exponierung zu vermeiden.

3.7 Microsoft SharePoint Server / SharePoint Services "help.aspx" Cross-Site Scripting

Risiko: problematisch
Remote: Ja
Datum: 30.04.2010
scip DB: http://www.scip.ch/?vuldb.4125

Windows SharePoint Services (kurz: WSS) bezeichnet ein Produkt der Firma Microsoft, das zum freien Herunterladen für Inhaber einer Windows-Server-Lizenz ab Version Windows Server 2003 verfügbar ist. Ziel der Windows SharePoint Services ist die virtuelle Zusammenarbeit von Benutzern unter einer Weboberfläche mit einer gemeinsamen Daten- und Informationsablage. Der grundlegende Aufbau der Windows SharePoint Services sorgt für eine integrative und themenorientierte Form der Zusammenarbeit zwischen den beteiligten Personen. Die Firma HTBridge veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Cross Site Scripting (XSS)) in verschiedenen Versionen des Produktes beschreibt. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:
Betroffenen Administratoren wird empfohlen, das Advisory von Microsoft zu diesem Thema zu konsultieren und entsprechende Gegenmassnahmen zu treffen.

3.8 HTC Touch Pro2 / HD2 SMS Preview Script Execution

Risiko: problematisch
Remote: Ja
Datum: 28.04.2010
scip DB: http://www.scip.ch/?vuldb.4124

Der HTC HD2, HTC-interner Codename Leo, ist ein Smartphone mit Windows Mobile 6.5 Betriebssystem, hergestellt von der HTC Corporation. Es ist das erste Windows Mobile Phone, das einen kapazitiven Touchscreen besitzt und das Multitouch unterstützt. Der Researcher Michael Müller der Firma Integralis veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Cross Site Scripting (XSS)) in verschiedenen Versionen des Produktes beschreibt. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

Expertenmeinung:
Auch hier handelt es sich um einen unschönen Fehler, bei der gerenderter Inhalt vor dessen Interpretierung nur unzureichend validiert wird. Auch hier sollte im Zweifelsfall der Hersteller im Hinblick auf eine Gegenmassnahme kontaktiert werden.

3.9 Palm Pre WebOS SMS Client Script Execution

Risiko: problematisch
Remote: Ja
Datum: 26.04.2010
scip DB: http://www.scip.ch/?vuldb.4122

webOS ist ein Smartphone-Betriebssystem der Firma Palm, das erstmals auf der Consumer Electronics Show 2009 am 8. Januar 2009 in Las Vegas vorgestellt wurde. Es stellt den Nachfolger des Palm OS dar und ist auf die Bedienung per kapazitivem Touchscreen angepasst. Der Name kommt von der engen Verflechtung mit dem Internet bzw. mit Internetdiensten. Ein Researcher der Intrepidus Group identifizierte unlängst eine Schwachstelle (Cross Site Scripting (XSS)) in aktuellen Versionen der vorliegenden Applikation. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

Expertenmeinung:
Die vorliegende Schwachstelle ist in erster Linie als unschön und alarmierend zu betrachten, da hier gewisse grundsätzliche Validierungsmassnahmen nicht getroffen wurden. Betroffene Benutzer sollten der Anleitung des Herstellers Folge leisten, um die Schwachstelle

zu mitigieren.

3.10 Internet Explorer XSS Filter Cross-Site Scripting

Risiko: problematisch
Remote: Ja
Datum: 26.04.2010
scip DB: http://www.scip.ch/?vuldb.4121

Der Internet Explorer (offiziell Windows Internet Explorer; früher Microsoft Internet Explorer; Abkürzung: IE oder MSIE) ist ein Webbrowser vom Softwarehersteller Microsoft für dessen Betriebssystem Windows. Seit Windows 95B ist der Internet Explorer fester Bestandteil dieser Betriebssysteme. Bei älteren Windows-Versionen kann er nachinstalliert werden. Die aktuelle Version ist Internet Explorer 8. Die Researcher David Lindsay ("thornmaker") und Eduardo A. Vela Nava ("sirdarckcat") veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Cross Site Scripting (XSS)) in verschiedenen Versionen des Produktes beschreibt. Der Angreifer kann durch die vorliegende Schwachstelle unter Umst„nden beliebigen Scriptcode zur Ausf• hrung bringen.

Expertenmeinung:
Die vorliegende Schwachstelle wird durch einen Fehler im XSS Filter des IE hervorgerufen. Die Schwachstelle kann zu einem gewissen Masse durch gewisse Konfigurationsänderungen mitigiert werden. Davon abgesehen sollte der Patch durch die Microsoft abgewartet und installiert werden.

3.11 Microsoft Windows "SfnLOGONNOTIFY()" und "SfnINSTRING()" Denial of Service

Risiko: problematisch
Remote: Nein
Datum: 23.04.2010
scip DB: http://www.scip.ch/?vuldb.4120

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 zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Ein unter dem Pseudonym MJ0011 an die ™ffentlichkeit getretener Researcher beschreibt in einem Advisory eine Schwachstelle (Denial of Service (DoS)) in aktuellen Versionen der Applikation. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und damit den Betrieb des Systems und der entsprechenden Umsysteme empfindlich stören.

Expertenmeinung:
Zur vorliegenden Schwachstelle sind nur unzureichende Daten vorhanden, was eine konkrete Einstufung schwierig macht. Es ist davon auszugehen, dass lediglich eine lokale Ausnutzung möglich ist. Für weitere Details sollte hier aber ein erweitertes Advisory des Herstellers oder einer Drittquelle abgewartet werden.

3.12 IBM DB2 Data Manipulation und Pufferüberlauf Schwachstelle

Risiko: problematisch
Remote: Teilweise
Datum: 23.04.2010
scip DB: http://www.scip.ch/?vuldb.4119

DB2 ist ein kommerzielles relationales Datenbank Management System (RDBMS) der Firma IBM, dessen Ursprünge auf das System R und die Grundlagen von E. F. Codd vom IBM Research aus dem Jahr 1970 zurückgehen. Die Firma IBM beschreibt in einem Advisory eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der Applikation. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

Expertenmeinung:
Die vorliegende Schwachstelle dürfte in den meisten Fällen, durch die fehlende Exponierung von DB2 Systemen nach aussen, nur als problematisch betrachtet werden. Dennoch sollte sie zeitnah bearbeitet werden, um eine Ausnutzung zu vermeiden.

3.13 VLC Media Player verschiedene Pufferüberlauf Schwachstellen

Risiko: kritisch
Remote: Ja
Datum: 22.04.2010
scip DB: http://www.scip.ch/?vuldb.4118

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. Das Entwicklerteam des popul„ren Mediaplayers identifizierte unlängst eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der vorliegenden Applikation. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:
Die vorliegenden Schwachstellen betreffen eine Vielzahl von Multimediaformaten, was grundsätzlich als kritisch zu betrachten ist. Wie so oft, ist hier das Einspielen der aktualisierten Softwareversion als beste Option zu betrachten, die zeitnah verfolgt werden sollte.

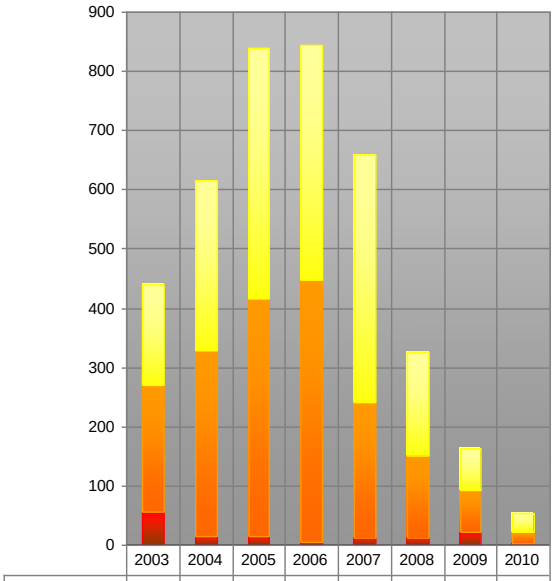
4. Statistiken Verletzbarkeiten

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

http://www.scip.ch/?vuldb

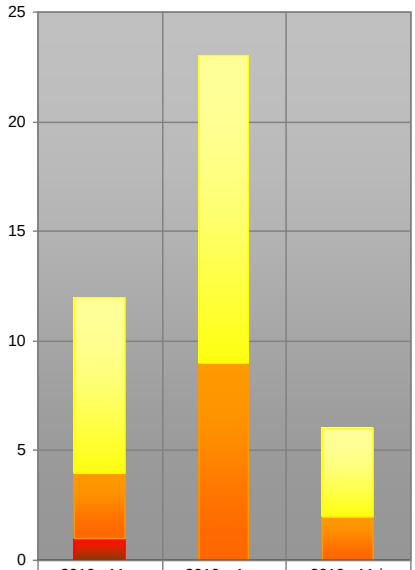
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an mailto:info@scip.ch. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum:	19. Mai 2010



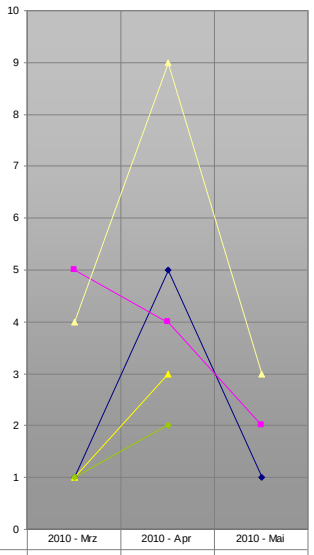
	2003	2004	2005	2006	2007	2008	2009	2010
problematisch	170	287	423	396	419	176	70	32
kritisch	214	314	402	442	229	140	72	19
sehr kritisch	56	15	15	6	11	11	21	3

Verlauf der Anzahl Schwachstellen pro Jahr



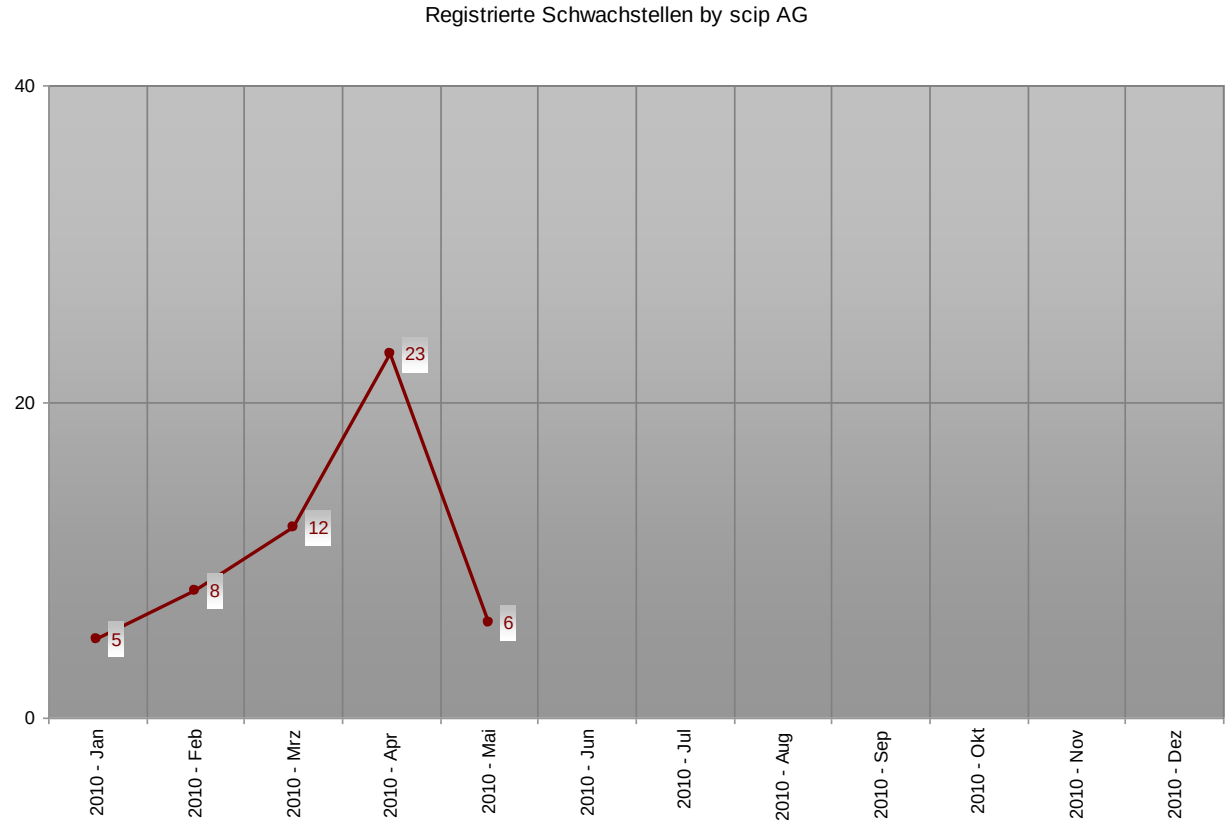
	2010 - Mrz	2010 - Apr	2010 - Mai
problematisch	8	14	4
kritisch	3	9	2
sehr kritisch	1		

Verlauf der letzten drei Monate Schwachstelle/Schweregrad

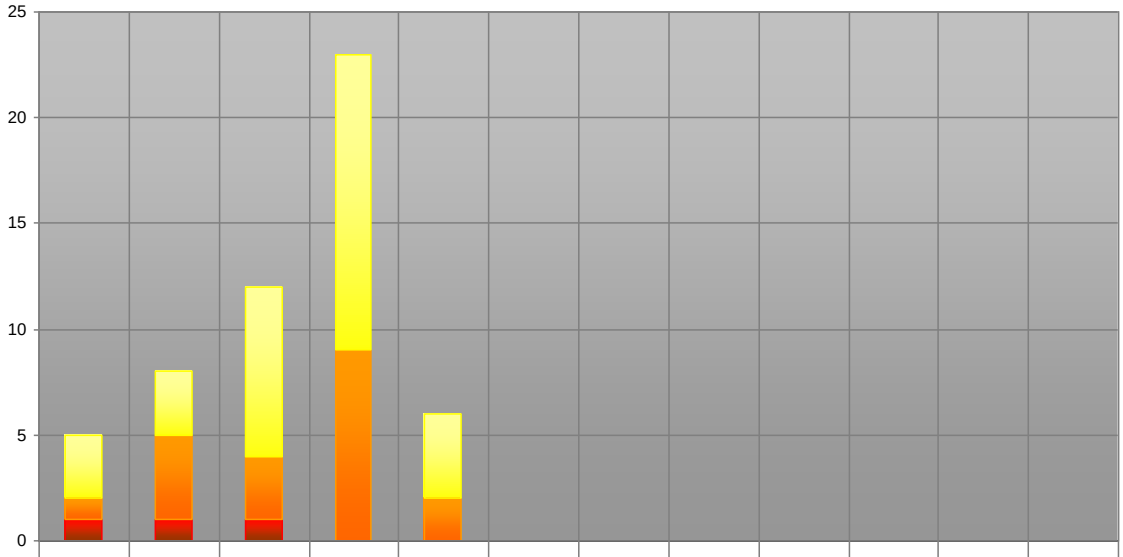


	2010 - Mrz	2010 - Apr	2010 - Mai
Cross Site Scripting (XSS)	1	5	1
Denial of Service (DoS)	5	4	2
Designfehler	1	3	
Directory Traversal			
Eingabeungültigkeit			
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Format String			
Konfigurationsfehler			
Pufferüberlauf	4	9	3
Race-Condition			
Schwache Authentifizierung			
Schwache			

Verlauf der letzten drei Monate Schwachstelle/Kategorie

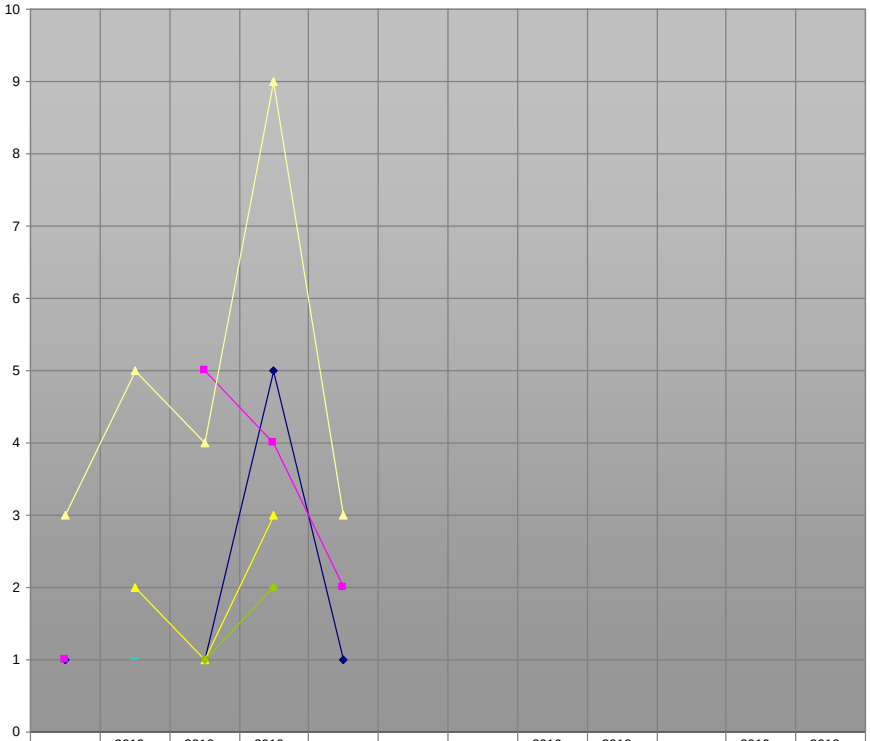


Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2010



	2010 - Jan	2010 - Feb	2010 - Mrz	2010 - Apr	2010 - Mai	2010 - Jun	2010 - Jul	2010 - Aug	2010 - Sep	2010 - Okt	2010 - Nov	2010 - Dez
problematisch	3	3	8	14	4							
kritisch	1	4	3	9	2							
sehr kritisch	1	1	1									

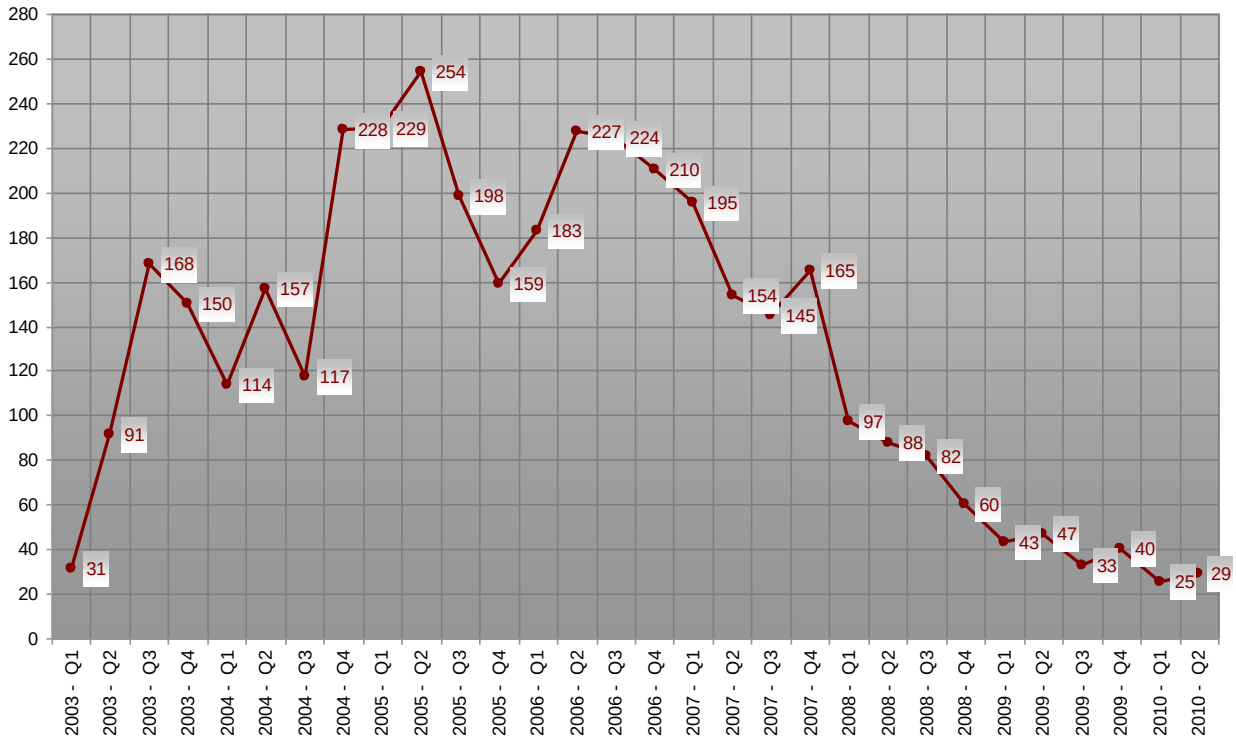
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2010



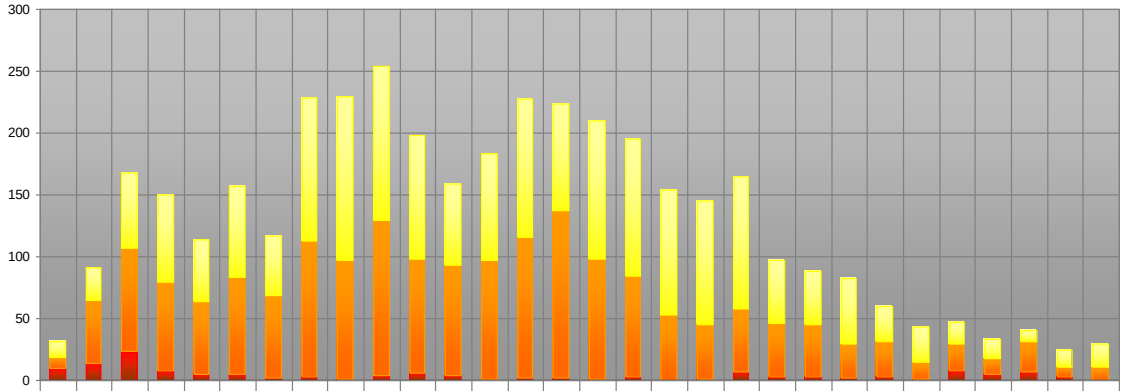
	2010 - Jan	2010 - Feb	2010 - Mrz	2010 - Apr	2010 - Mai	2010 - Jun	2010 - Jul	2010 - Aug	2010 - Sep	2010 - Okt	2010 - Nov	2010 - Dez
Cross Site Scripting (XSS)	1		1	5	1							
Denial of Service (DoS)	1		5	4	2							
Designfehler		2	1	3								
Directory Traversal												
Eingabeungültigkeit												
Fehlende Authentifizierung												
Fehlende Verschlüsselung												
Fehlerhafte Leserechte												
Fehlerhafte Schreibrechte												
Format String												
Konfigurationsfehler												
Pufferüberlauf	3	5	4	9	3							
Race-Condition												
Schwache Authentifizierung												
Schwache Verschlüsselung												
SQL-Injection												
Symlink-Schwachstelle												
Umgehungs-Angriff		1										
Unbekannt			1	2								

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2010

Registrierte Schwachstellen by scip AG

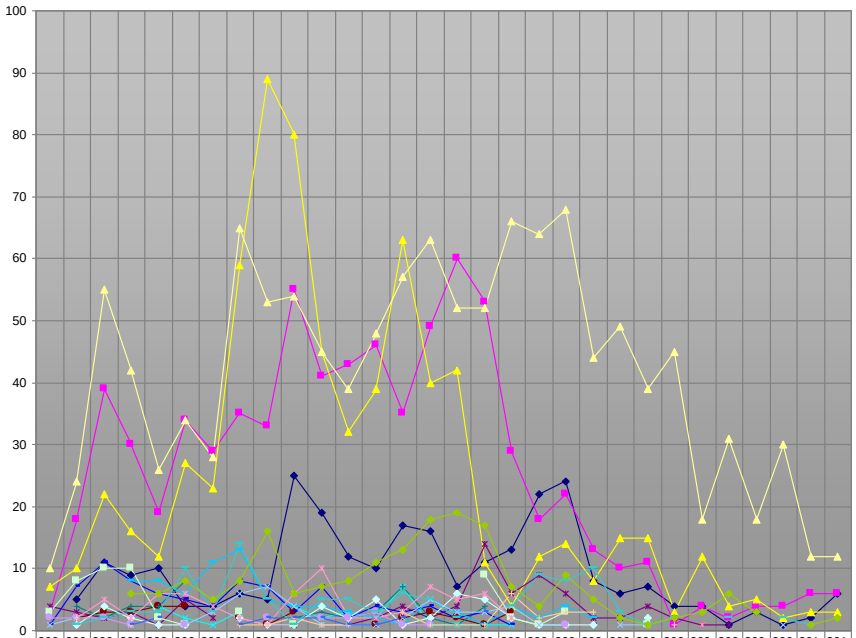


Verlauf der Anzahl Schwachstellen pro Quartal seit 2003 Q1



	2003 - Q1	2003 - Q2	2003 - Q3	2003 - Q4	2004 - Q1	2004 - Q2	2004 - Q3	2004 - Q4	2005 - Q1	2005 - Q2	2005 - Q3	2005 - Q4	2006 - Q1	2006 - Q2	2006 - Q3	2006 - Q4	2007 - Q1	2007 - Q2	2007 - Q3	2007 - Q4	2008 - Q1	2008 - Q2	2008 - Q3	2008 - Q4	2009 - Q1	2009 - Q2	2009 - Q3	2009 - Q4	2010 - Q1	2010 - Q2
problematisch	12	26	61	71	50	74	48	115	132	125	100	66	86	111	87	112	111	101	100	107	51	43	53	29	28	18	15	9	14	18
kritisch	9	51	83	71	59	78	67	110	96	125	92	89	96	114	135	97	81	53	44	51	43	42	27	28	14	21	13	24	8	11
sehr kritisch	10	14	24	8	5	5	2	3	1	4	6	4	1	2	2	1	3		1	7	3	3	2	3	1	8	5	7	3	

Verlauf der Anzahl Schwachstellen/Schweregrad pro Quartal seit 2003 Q1



	2003-Q1	2003-Q2	2003-Q3	2003-Q4	2004-Q1	2004-Q2	2004-Q3	2004-Q4	2005-Q1	2005-Q2	2005-Q3	2005-Q4	2006-Q1	2006-Q2	2006-Q3	2006-Q4	2007-Q1	2007-Q2	2007-Q3	2007-Q4	2008-Q1	2008-Q2	2008-Q3	2008-Q4	2009-Q1	2009-Q2	2009-Q3	2009-Q4	2010-Q1	2010-Q2
Cross Site Scripting (XSS)		5	11	9	10	4	4	6	5	25	19	12	10	17	16	7	11	13	22	24	8	6	7	4	4	1	3	1	2	6
Denial of Service (DoS)	3	18	39	30	19	34	29	35	33	55	41	43	46	35	49	60	53	29	18	22	13	10	11	1	4	2	4	4	6	6
Designfehler	7	10	22	16	12	27	23	59	89	80	45	32	39	63	40	42	11	4	12	14	8	15	15	3	12	4	5	2	3	3
Directory Traversal					4	2	1	3		4	2	3	2	7	1	1	1	1												
Eingabeungültigkeit	4	3	2	3	1	5	2		1	1		1	2	4	2	4	14	6	9	6	2	2	4	2	1	1				
Fehlende Authentifizierung		2	3	3	4	4		2	1	3			1	2	3	2	1	3												
Fehlende Verschlüsselung		4	2	4	4	8				2	3	2	3	7	2	1	4													
Fehlerhafte Leserechte	1	7	11	8	6	5	4	8	7	3	7	2	4	3	4	2	3	1			1									
Fehlerhafte Schreibrechte				8	8	6	11	13	5	4	4	3	2	1	5	3	1	4	2	4	2									
Format String		1	4	2	1	1		2	1	1	4	2	5	1	2	6	5	2	1	1	1		2							
Konfigurationsfehler	3	8	10	10	2	1		3		1							9	2	1	3			1							
Pufferüberlauf	10	24	55	42	26	34	28	65	53	54	45	39	48	57	63	52	52	66	64	68	44	49	39	45	18	31	18	30	12	12
Race-Condition	1	2		1		1	3	6	7	4	1	1	1	2	5	3	3	4	1	1		1	1					1		
Schwache Authentifizierung		2	5	2	6	6	4	2	1	6	10	2	2	3	7	5	6	2		1					1					
Schwache Verschlüsselung	2	2	2	1		1			2		2	2	3	1	1					1										
SQL-Injection		2		1				1	1	2	1	1		3	1	1	1	6	2	3	3			1						
Symlink-Schwachstelle				1	2			1	2	2	2	1	1	2			3													
Umgehungs-Angriff		1	2	3	3	10	3	14	5	1	5	5	3	6	5	2		4	9	8	10	3	1	2		2		2	1	
Unbekannt				6	6	8	5	8	16	6	7	8	11	13	18	19	17	7	4	9	5	2	1	2	3	6	3		1	2

Verlauf der Anzahl Schwachstellen/Kategorie pro Quartal seit 2003 Q1

5. Labs

Auf der scip Labs Webseite (http://www.scip.ch/?labs.archiv) werden regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

5.1 Technische Bild-Forensik

19.03.2010 Marc Ruef, maru@scip.ch

Der Bereich der Forensik ist vielfältig. Im Rahmen dessen geht es jeweils um das Identifizieren von verborgenen Informationen und dem Erkennen von Zusammenhängen. Zum Beispiel kann versucht werden mittels Carving einzelne Dateien aus einem Datenträger zu extrahieren. Oder durch das Analysieren von Netzwerkkommunikationen kann versucht werden einen Angriff als solchen zu erkennen.

Der Bereich der Bild-Forensik ist nicht minder spannend. Zwei Mechanismen sollen nachfolgend vorgestellt werden. Sie helfen dabei Hinweise auf die Herkunft eines digitalen Fotos zusammenzutragen. Zum Zweck dieser Untersuchung wurde ein beliebiges Foto aus dem Internet heruntergeladen und analysiert. Es wird anbei dargestellt.

Exif-Tags – Bildinformationen auslesen
Das Exchangeable Image File Format ist ein Standard der Japan Electronic and Information Technology Industries Association (JEITA) für das Dateiformat, in dem moderne Digitalkameras Informationen über die aufgenommenen Bilder speichern.

Diese Metadaten enthalten grundlegende Details, die für eine Analyse von Interesse sein kann. Nachfolgend werden die vom Original-Bild extrahierten Exif-Daten dargestellt. Zu einem jeden Tag wird ein entsprechender Value bereitgestellt. Es werden nur die im Rahmen einer forensischen Untersuchung besonders interessanten Werte dargelegt.

Exif-Tag	Information
Make	KONICA MINOLTA CAMERA, Inc.
Model	DiMAGE G400
DateTimeOriginal	2006:07:08 12:49:17
DateTimeDigitized	2006:07:08 12:49:17
Flash	Flash not fired, auto mode
DigitalZoomRatio	0.00 x
SceneCaptureType	Standard
Exif-Tag	Information
Subject-DistanceRange	Unknown

Zum Beispiel wird im Tag Make der Name des Herstellers der Kamera, die für die Aufnahme herangezogen wurde, ausgewiesen. Zusätzlich findet sich in Model die Modellbezeichnung des Geräts. So wurde für die besagte Aufnahme eine Konica Minolta DiMAGE G400 verwendet. Der Zeitpunkt der Aufnahme als solche wird im Tag `DateTimeOriginal` abgelegt. Sie erfolgte damit am *2006/07/08 um 12:49 Uhr* (Wir haben als Fallbeispiel absichtlich ein etwas älteres Foto genommen).

Ebenso finden sich einige grundlegenden technischen Informationen zur Konfiguration der Kamera. Zum Beispiel in `Flash`, ob ein Blitz verwendet, in `Contrast`, ob Anpassungen am Kontrast vorgenommen und in `DigitalZoomRatio`, welche Ratio des digitalen Zooms verwendet wurden.

Längerfristig werden vor allem GPS-Informationen, wie sie in den Tags `GPSLatitude` und `GPSLongitude` abgelegt werden, von Interesse sein. Gerade weil immer mehr Kameras einen entsprechenden GPS-Chip mitbringen und die Daten auch entsprechend taggen – So zum Beispiel das iPhone 3GS. Gerade anonyme Bilder, wie sie zum Beispiel in Erotik-Inseraten verbreitet werden, können so unter Umständen Rückschluss auf die Personendaten zulassen. Eine erste statistische Analyse in dieser Richtung im Zusammenhang mit Twitpic wurde von Johannes Ullrich publiziert.

Thumbnails – Originalbilder erkennen
Viele Kameras und Bildbearbeitungsprogramme speichern in den jeweiligen Bildern ein Thumbnail ab. Hierbei handelt es sich um eine kleinere Version des Bilds, die beispielsweise bei einer gekachelten Übersicht herangezogen werden kann. Da nur ein kleines Bild dargestellt werden will, muss auch nur eine kleine Version mit erheblich hoher Geschwindigkeit geladen werden (z.B. 120×90 anstatt 1280×960).

Oftmals werden Bilder weiterverarbeitet, ohne das Thumbnail des Original-Bilds anzupassen bzw. zu löschen. Erstmals grosse Aufmerksamkeit erlangte dieser Effekt, als die TechTV-Moderatorin Catherine Schwartz vermeintliche Portraitfotos von sich online stellte. Im Thumbnail des Bilds war jedoch klar zu sehen, dass dies ursprünglich eine Ganzkörperaufnahme mit ohne Kleidung war.

Dieser Effekt soll nun an nachfolgender Bildserie

illustriert werden. Als erstes wird das effektive Original-Bild dargestellt, das als Thumbnail abgelegt wurde. Bei der Bildbearbeitung wurde sich entschieden, den im zweiten Bild markierten Bereich auszuschneiden und als neues Originalbild in der dritten Abbildung (Hund im Wasser) einzusetzen. Indem nun das Thumbnail des neuen Originalbilds extrahiert werden konnte, liess sich das effektive Originalbild (Mann mit Hund) ausmachen:

Der Finne Tõnu Virolaismies Samuel bietet auf seiner Webseite einen auf PHP basierenden Crawler an, der automatisiert derlei Thumbnails ausmachen kann. In der Gallery sind einige schöne Beispiele dafür zu sehen, wie sich bisweilen ganz kuriose Originalbilder ausmachen lassen. Eric Schmidt, der CEO von Google hat diesen Effekt mit folgenden Worten abgetan.

If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place.

6. Impressum

Herausgeber:

)SCIP(scip ag
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 Information 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 beschäftigen. 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 Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. Anmelden! Abmelden!