

## Contents

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

### 1. Editorial

#### Das Pentesting Experten System

Seit meinem Eintritt in den Bereich der Netzwerksicherheit haben mich Vulnerability Scanner zur automatisierten Identifikation von Sicherheitslücken fasziniert. Erste Gehversuche mit einer eigenen Implementierung habe ich im Jahr 2000 mit dem Dante Projekt umgesetzt. Der auf modularen Shell-Skripten basierende Security Scanner sollte über eine Weboberfläche bedienbar und deshalb durch jedermann benutzbar sein.

Rund vier Jahre später habe ich mit einer konkreten Implementierung für das Attack Tool Kit (ATK) begonnen. Dieses sollte noch einen Schritt weitergehen und neben dem Identifizieren von Schwachstellen eben jene auch gleich Ausnutzbar machen. Dies geschah in jener Zeit, als das MetaSploit Framework (MSF) entwickelt und damit der Begriff des Exploiting Frameworks geprägt wurde.

Sowohl Dante als auch das ATK sollten mir bei meiner täglichen Arbeit als Penetration Tester helfen können. Sie sollten mich dabei unterstützen, Sicherheitsüberprüfungen automatisiert durchführen zu lassen. Dadurch sollte sich sowohl die Effizienz als auch die Qualität der Tests erhöhen lassen. Dies ist, natürlich unter Miteinbezug vergleichbarer Lösungen wie Nessus und Qualys, möglich gewesen. Doch nie habe ich mich so richtig wohl

mit diesem Flickwerk aus Werkzeugen gefühlt.

Ein ursprünglich mit dem Arbeitstitel ATK.NET angefangenes Projekt sollte die Defizite bestehender Produkte, und dazu zählen selbstverständlich auch meine Ansätze, eliminiert werden. Diese Lösung sollte sowohl die Möglichkeiten eines umfangreichen Vulnerability Scanners, als auch eines intelligenten Fuzzing-Tools sowie eines Exploiting-Frameworks bieten. Eine Analyse sollte sich dabei in unterschiedlicher Genauigkeit (diese hat ebenso Auswirkungen auf die Dauer der Ausführung) als auch in unterschiedlichen und stufenlosen Graden an Automatisierung durchführen lassen (von nahezu manuellen Tests bis hin zu komplett automatisierten Scans).

Insgesamt 10 Jahre meiner Entwicklungszeit wurde in diese Lösung investiert. Davon über 8 Jahre zusammen mit meinen hervorragenden Arbeitskollegen bei scip AG. Durch eine hochgradig modulare Lösung sehen wir uns in der Lage, anhand eines Expertensystems unsere hochgesteckten Ziele zu erreichen. Wir vereinen dabei die Möglichkeiten der unterschiedlichen Lösungsansätze, ohne auf Flexibilität verzichten zu müssen.

Wir unterscheiden dabei zwischen verschiedenen Engines. Die Scan-Engine ist für das (semi-)automatisierte Zusammentragen der potentiellen und ausgemachten Schwachstellen verantwortlich. Dabei wird in einer ersten Phase versucht, den grundlegenden Aufbau eines überprüften Objekts (Netzwerk, System, Dienst, Applikation oder Daten) zu identifizieren. Anhand verschiedener Mechanismen wird versucht die eingesetzten Technologien und die angewandten Konfigurationseinstellungen auszumachen. Da es sich hierbei um dynamische Module handelt, lassen sich damit auch komplett unbekannte Lösungen und Eigenentwicklungen analysieren.

Die durch die Scan-Engine gesammelten und als XML-Dateien bereitgestellten Daten werden durch einen Parser bearbeitet. Im Pre-Parsing wird es möglich, anhand der ermittelten Mechanismen erste statistische Auswertungen vorzutragen. Da das Parsing besonders effizient umgesetzt wird, lässt sich dies in Echtzeit an den Scanning-Prozess knüpfen. Theoretisch kann

der Kunde in jedem Augenblick eines Projekts über den aktuellen Stand informiert werden.

Das Pre-Parsing erlaubt jedoch ebenfalls eine erste Moderation der Resultate. Damit kann Einfluss auf den iterativen Prozess des Scannings, aber auch auf die Weiterverarbeitung der gesammelten Daten, ausgeübt werden. Zum Beispiel lassen sich On-The-Fly neue Tests generieren, bekannte False-Positives markieren (Flagging) oder weiterführende Validierungen anstreben.

Durch das effektive Parsing werden die Daten in eine Datenbank geschrieben. Dort lassen sich erste Planspiele anstreben. Durch statistische Auswertungen können Hochrechnungen für die anstehenden Tests getätigt werden. Oder es lassen sich Delta- sowie Trendanalysen, auf der Basis vorangegangener Sicherheitsüberprüfungen des gleichen Kunden oder vergleichbarer Kunden, umsetzen.

Werden die Daten in der Datenbank abgelegt, kann eine feste Moderation umgesetzt werden. Dabei erlaubt das System eine durch unterschiedliche Analysten in unabhängiger Weise umgesetzte Moderation. Es können also verschiedene Leute die Einträge kontrollieren, beglaubigen und validieren. Dies müssen nicht zwingend die gleichen Personen sein, die die initialen Scans durchgeführt haben. Damit lässt sich ebenso ein Vieraugenprinzip anwenden, indem potentielle Schwachstellen nur dann als gegeben akzeptiert werden, wenn mindestens zwei Auditoren ihr "Accepted" abgegeben haben.

Die Datenbank fungiert sodann als Expertensystem. Dieses weist die Analysten darauf hin, wie hoch die Chancen für False-Positives (und False-Negatives) sind, wie sich diese erkennen und eliminieren lassen. Durch Schritt-für-Schritt Anleitungen bzw. dynamisch generierte Scan-scripte können sodann weiterführende Tests oder Validierungen durchgeführt werden. Der Tester muss sodann nicht zwingend im Detail mit der Zielumgebung und den eingesetzten Technologien vertraut sein, da er sich auf den gesammelten Erfahrungsschatz unseres Unternehmens bzw. der anderen Analysten verlassen kann.

Dieser Prozess des Prüfen, Validieren, Parsen, Moderieren und Dokumentieren kann iterativ und beliebig oft wiederholt werden. Zu jedem Zeitpunkt sind sämtliche Daten vorhanden und können auf Knopfdruck ausgegeben werden (Report, Statistiken, Trends). In der Regel wird ein Ablauf der Form Scan-Moderation-Scan-Moderation-Dokumentation angestrebt. Dadurch

kann gewährleistet werden, dass Schwachstellen, die bei den ersten Tests nicht identifiziert werden konnten (da sämtliche Angriffsflächen so noch nicht bewusst waren) doch noch identifiziert werden können.

In der Datenbank werden umfangreiche Informationen zu den jeweiligen Schwachstellen abgelegt. Neben einer Charakterisierung des Problems findet sich ebenfalls mindestens eine Schritt-für-Schritt Anleitung zur Ausnutzung des Problems und verschiedene Gegenmassnahmen (priorisiert nach ihrer Effektivität). Ebenso wird eine umfangreiche Attributisierung durchgesetzt. So werden Phase eines Angriffs (z.B. Auswertung), Angreifertyp (z.B. Skript-Kiddie), Schwachstellenklasse (z.B. Cross Site scripting), betroffenes Objekt (z.B. Webapplikation) und Parent-Bug (die für die Existenz dieser Schwachstelle erforderliche Voraussetzung) festgehalten. Zusätzlich sind Referenzen auf andere Scanner (inklusive deren Beschreibungen, Einstufungen und Testverfahren), Verwundbarkeitsdatenbanken, Webseiten und Bücher in dieser Wissensdatenbank festgehalten.

Werden sämtliche Daten in der Datenbank eingetragen und moderiert, kann ein Report generiert werden. Durch die umfangreiche Report-Engine wird es möglich, verschiedene Ausgabeformen und Dateiformate zu unterstützen. Dies reicht von klassischen Word-/PDF-Reports mit allen Details über Excel-Dokumente mit den wichtigsten Gegenmassnahmen (Checklisten) bis hin zu XML-Dateien zur automatisierten Weiterverarbeitung (z.B. in einem Bugtracking-System).

Das grundlegende Ziel des Reportings ist dabei, keine der gesammelten und vorhandenen Informationen zu verlieren. In einem Report sind also stets alle Daten enthalten, die von Nutzen sind. Zu jeder gefundenen Schwachstelle werden projektbezogene Informationen, wie die IP-Adresse des Scan-Systems und der Zeitpunkt der Identifikation, bereitgestellt. Damit kann ein Höchstmass an Transparenz und Nachvollziehbarkeit gewährleistet werden. Ganze Tests lassen sich also auch nach Abschluss bis auf die Sekunde genau rekonstruieren.

Marc Ruef <maru-at-scip.ch>  
Security Consultant  
Zürich, 26. Juli 2010



## 2. scip AG Informationen

### 2.1 Wir stellen ein

Hervorragende Leistung kann nur durch ein hervorragendes Team entstehen. Die scip AG verfolgt seit ihrer Gründung in 2002 eine konstante, qualitätsorientierte Personalpolitik, bei der die Nutzung und Förderung individueller Fähigkeiten und Talente im Vordergrund steht.

Zur Erweiterung unseres Teams suchen wir:

- Security Consultant (Senior) - 100%
- Security Consultant (Junior) - 100%

Die Umsetzung unserer Kunden-Projekte verlangt ein Höchstmass an Fachwissen.

Überzeugen Sie uns!

Details zu unserem eigenen Recruitment Prozess und wie Sie uns überzeugen können, dass Sie genau der oder die Richtige sind, finden Sie unter:

<http://www.scip.ch/?firma.jobs>

Selbstverständlich werden alle Eingänge streng vertraulich behandelt.

### 2.2 Security Coaching

Das Ziel des Security Coaching ist die direkte Beratung und das unmittelbare Coaching des Kunden in den Bereichen der Information Security zur Sicherstellung nachhaltiger und sicherer Prozesse, Architektur- und Technologieentscheidungen.

Der Kunde bespricht mit uns seine Ziele und Vorgaben. Anhand dessen unterstützen wir den Kunden mit unserer fachmännischen Expertise und langjährigen Erfahrung im Security Bereich. Bei Sitzungen mit Partnern stellen wir das entsprechende Know-How zur Formulierung wichtiger Nachfragen zur Verfügung.

- Vorbereitung: Zusammentragen aller vorhandenen Informationen zur 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 vertretbaren Lösungswegs.

In erster Linie soll in beratender Weise eine direkte Hilfestellung mit konkreten Empfehlungen und Lösungen bereitgestellt werden. Eine Dokumentation (Protokolle, Kommunikationsmatrizen, Statements etc.) erfolgt auf Wunsch des Kunden.

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

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen konnten wir als scip AG bereits eine grosse Anzahl an Kunden beraten und begleiten.

Zählen auch Sie auf uns!

<http://www.scip.ch/?firma.referenzenalle>

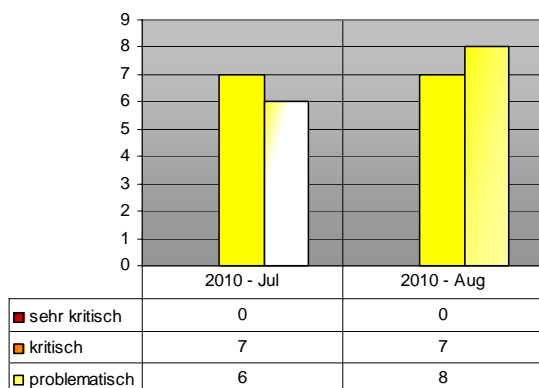
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an [chris.widmer@scip.ch](mailto:chris.widmer@scip.ch).

### 3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/?vuldb> einsehbar.



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



#### Contents:

- 4171 Apple Safari verschiedene Schwachstellen
- 4170 Cisco IOS TCP Connection Handling Denial of Service
- 4169 Adobe ColdFusion Directory Traversal Schwachstelle
- 4167 Microsoft Windows MPEG Layer-3 Audio Decoder Pufferüberlauf
- 4166 Microsoft Windows SMB Server verschiedene Schwachstellen
- 4165 Windows TCP/IP Implementation Denial of Service/Privilege Escalation
- 4164 Microsoft Internet Explorer mehrere Schwachstellen
- 4163 Microsoft XML Core Services Invalid HTTP Response Handling Schwachstelle
- 4162 Microsoft Windows Kernel Denial of Service/Privilege Escalation
- 4161 Microsoft Windows TLS/SSL Session Renegotiation Plaintext Injection Schwachstelle
- 4160 Microsoft .NET Framework / Silverlight verschiedene Code Execution Schwachstellen
- 4159 Microsoft Office Excel SXDB Record Parsing Pufferüberlauf
- 4157 Foxit Reader FreeType2 CFF Font Parsing Schwachstelle
- 4156 Apple iOS CFF Font Parsing and IOSurface Integer Overflow

4155 Google Chrome verschiedene Schwachstellen

#### 3.1 Apple Safari verschiedene Schwachstellen

Risiko: **kritisch**

Remote: Ja

Datum: 22.07.2010

scip DB: <http://www.scip.ch/?vuldb.4171>

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, seit Version 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. Die Firma Apple beschreibt eine Reihe von Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

#### Expertenmeinung:

Die vorliegende Schwachstelle kann durchaus kritisch Auswirkungen nach sich ziehen. Betroffene Systeme sollten daher zeitnah gepatcht werden, um eine Kompromittierung zu vermeiden.

#### 3.2 Cisco IOS TCP Connection Handling Denial of Service

Risiko: **problematisch**

Remote: Ja

Datum: 13.08.2010

scip DB: <http://www.scip.ch/?vuldb.4170>

Internetwork Operating System Software (IOS) ist das Betriebssystem von Cisco-Routern und -Switches. Das Betriebssystem geht zurück auf den Angestellten der Stanforder Medizinischen Schule namens Bill Yeager, der um 1980 die Software entwickelte, welche es den Routern ermöglicht, Netzwerke unterschiedlicher Medien und Protokolle miteinander zu verbinden. Er arbeitete bis 1984 mit Sandra Lerner und Len Bock, den Gründern von Cisco, an der Verbesserung dieser Software zusammen. Mit der Gründung von Cisco im Jahre 1984 lizenzierte Cisco diese Software von Yeager. Seitdem wurde sie in verschiedenen Versionen eingesetzt und liegt seit Oktober 2009 in der Version 15.0 vor. Die Firma Cisco veröffentlichte unlängst verschiedene Schwachstellen,

vornehmlich der Kategorie Denial of Service (DoS) in verschiedenen Versionen des Produktes. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und damit den Betrieb des Systems und der entsprechenden Um Systeme empfindlich stören.

#### Expertenmeinung:

Diese Schwachstelle ist zwar nicht hochkritisch, kann aber je nach Umgebung und Art des Angriffs durchaus kritische Folgen haben. Betroffene Systeme sollten zeitnah mit Patches versorgt werden.

### 3.3 Adobe ColdFusion Directory Traversal Schwachstelle

Risiko: **problematisch**

Remote: Ja

Datum: 11.08.2010

scip DB: <http://www.scip.ch/?vuldb.4169>

ColdFusion ist eine für Web-basierte Datenbank-Anwendungen konzipierte Middleware des Software-Herstellers Adobe Systems, die grundlegend aus den folgenden drei Teilen besteht: 1. ColdFusion Application Server, 2. ColdFusion Markup Language (CFML, eine Skriptsprache, die es ermöglicht, serverseitige Applikationen zu programmieren), 3. geeignete Entwicklungsumgebungen (wie zum Beispiel Eclipse oder Dreamweaver). ColdFusion steht dabei in direkter Konkurrenz zu vergleichbaren serverseitigen Systemen wie ASP.NET, JSP/Servlet, Ruby on Rails (RoR), ZOPE (Python), Perl und PHP. Im Gegensatz zu Skriptsprachen wie Perl, PHP, Python und Ruby, die Open Source sind, ist die Originalversion von ColdFusion nicht im Quellcode verfügbar. Der Researcher Richard Brain der Firma ProCheckUp Ltd. identifizierte unlängst eine Schwachstelle (Directory Traversal) in aktuellen Versionen der vorliegenden Applikation. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

#### Expertenmeinung:

Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah gepatcht werden.

### 3.4 Microsoft Windows MPEG Layer-3 Audio Decoder Pufferüberlauf

Risiko: **kritisch**

Remote: Nein

Datum: 10.08.2010

scip DB: <http://www.scip.ch/?vuldb.4167>

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 Moritz Jodeit veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Pufferüberlauf) 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:

Während diese Schwachstelle nicht zwingend kritisch ist, sollte aufgrund des verbleibenden Restrisikos das zeitnahe Einspielen entsprechender Patches angestrebt werden.

### 3.5 Microsoft Windows SMB Server verschiedene Schwachstellen

Risiko: **problematisch**

Remote: Ja

Datum: 10.08.2010

scip DB: <http://www.scip.ch/?vuldb.4166>

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. Die Firma Microsoft beschreibt eine Reihe von Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

#### Expertenmeinung:

Die vorliegende Schwachstelle kann durchaus kritische Auswirkungen nach sich ziehen. Betroffene Systeme sollten daher zeitnah

gepatcht werden, um eine Kompromittierung zu vermeiden

### 3.6 Windows TCP/IP Implementation Denial of Service/Privilege Escalation

Risiko: **problematisch**  
Remote: Ja  
Datum: 10.08.2010  
scip DB: <http://www.scip.ch/?vuldb.4165>

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. Eine Gruppe von Researchern 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:

Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah gepatcht werden.

### 3.7 Microsoft Internet Explorer mehrere Schwachstellen

Risiko: **kritisch**  
Remote: Ja  
Datum: 10.08.2010  
scip DB: <http://www.scip.ch/?vuldb.4164>

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. Ein Kollektiv von Researchern beschreibt eine Reihe von Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

#### Expertenmeinung:

Diese Schwachstelle ist zwar nicht hochkritisch, kann aber je nach Umgebung und Art des Angriffs durchaus kritische Folgen haben. Betroffene Systeme sollten zeitnah mit Patches versorgt werden

### 3.8 Microsoft XML Core Services Invalid HTTP Response Handling Schwachstelle

Risiko: **kritisch**  
Remote: Ja  
Datum: 10.08.2010  
scip DB: <http://www.scip.ch/?vuldb.4163>

Microsoft XML Core Services (MSXML) ist eine Softwarebibliothek, die die Entwicklung von nativen Windows-Programmen mit XML-Unterstützung in den Programmierumgebungen JScript, VBScript und anderen Microsoft-Entwicklungsumgebungen erlaubt. Sie unterstützt XML in der Version 1.0, DOM, SAX, XSLT, XML Schemata in XSD und XDR, sowie andere zu XML gehörende Technologien. Die Firma Google beschreibt in einem Advisory eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der Applikation. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

#### Expertenmeinung:

Während diese Schwachstelle nicht zwingend kritisch ist, sollte aufgrund des verbleibenden Restrisikos das zeitnahe Einspielen entsprechender Patches angestrebt werden.

### 3.9 Microsoft Windows Kernel Denial of Service/Privilege Escalation

Risiko: **problematisch**  
Remote: Ja  
Datum: 10.08.2010  
scip DB: <http://www.scip.ch/?vuldb.4162>

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 Tavis Ormandy beschreibt eine

Reihe von Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. 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 als kritisch zu betrachten und sollte zeitnah gepatcht werden

### 3.10 Microsoft Windows TLS/SSL Session Renegotiation Plaintext Injection Schwachstelle

Risiko: **problematisch**

Remote: Ja

Datum: 10.08.2010

scip DB: <http://www.scip.ch/?vuldb.4161>

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. Die Firma PhoneFactor veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Designfehler) in verschiedenen Versionen des Produktes beschreibt. Die Schwachstelle erlaubt es dem Angreifer XSS (Cross Site Scripting) Angriffe durchzuführen und dadurch beliebigen Kontext im Browser des Opfers zur Ausführung zu bringen.

#### Expertenmeinung:

Mit der vorliegenden Schwachstelle reiht Microsoft verschiedene seiner Produkte in eine ziemlich lange Liste von, durch SSL Renegotiation Schwachstellen betroffenen, Applikationen ein. Betroffene Systeme sollten mit entsprechenden Gegenmassnahmen und Patches versorgt werden.

### 3.11 Microsoft .NET Framework / Silverlight verschiedene Code Execution Schwachstellen

Risiko: **kritisch**

Remote: Ja

Datum: 10.08.2010

scip DB: <http://www.scip.ch/?vuldb.4160>

.NET bezeichnet eine von Microsoft entwickelte Software-Plattform zur Entwicklung und Ausführung von Programmen. Sie besteht aus einer Laufzeitumgebung (für die Ausführung von Programmen) sowie einer Sammlung von Klassenbibliotheken, Programmierschnittstellen und Dienstprogrammen (Services). .NET ist im vollen Umfang nur für Windows verfügbar. Viele Programme laufen mit Hilfe des Mono-Projektes auf Unix basierten Betriebssystemen. Ein Researcher der Mozilla Corporation veröffentlichte unlängst verschiedene Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

#### Expertenmeinung:

Diese Schwachstelle ist zwar nicht hochkritisch, kann aber je nach Umgebung und Art des Angriffs durchaus kritische Folgen haben. Betroffene Systeme sollten zeitnah mit Patches versorgt werden.

### 3.12 Microsoft Office Excel SXDB Record Parsing Pufferüberlauf

Risiko: **kritisch**

Remote: Ja

Datum: 10.08.2010

scip DB: <http://www.scip.ch/?vuldb.4159>

Microsoft Excel ist das am weitesten verbreitete Tabellenkalkulationsprogramm. Excel gehört zur Microsoft-Office-Suite und ist sowohl für Microsoft Windows als auch für Mac OS verfügbar. Excel entstand als Nachfolger von Microsoft Multiplan. Die aktuelle Version ist für Windows Microsoft Excel 2010 und für Mac OS Microsoft Excel 2008. Der Researcher Damian Frizza der Firma CORE 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 vorliegende Schwachstelle kann durchaus kritisch Auswirkungen nach sich ziehen. Betroffene Systeme sollten daher zeitnah gepatcht werden, um eine Kompromittierung zu vermeiden.

### 3.13 Foxit Reader FreeType2 CFF Font

## Parsing Schwachstelle

Risiko: **kritisch**  
 Remote: Ja  
 Datum: 06.08.2010  
 scip DB: <http://www.scip.ch/?vuldb.4157>

Foxit Reader ist eine kostenlose Software zum Anzeigen von PDF-Dateien und somit eine Alternative zum weitverbreiteten Adobe Reader. Entwickelt wurde das Programm von der im US-Bundesstaat Kalifornien ansässigen Firma "Foxit Software". Eine größere Bekanntheit erreichte es vor allem nach dem Erscheinen der Version 6 des Adobe Readers, die von vielen Anwendern wegen der langen Ladezeiten kaum benötigter Plugins kritisiert wurde. Anders als z. B. "Sumatra PDF" ist Foxit Reader jedoch nicht quelloffen. Die Firma Foxit 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 ist als kritisch zu betrachten und sollte zeitnah gepatcht werden.

## Schwachstellen

Risiko: **kritisch**  
 Remote: Ja  
 Datum: 27.07.2010  
 scip DB: <http://www.scip.ch/?vuldb.4155>

Google Chrome ist ein Webbrowser, der von Google Inc. entwickelt wird und seit dem 2. September 2008 verfügbar ist. Am 11. Dezember 2008 erschien die erste finale Version. Zentrales Konzept ist die Aufteilung des Browsers in optisch und auf Prozessebene getrennte Browser-Tabs. Google Chrome baut auf der Rendering-Engine WebKit auf, die ihrerseits aus dem KDE-Projekt KHTML hervorging und auch in Apples Browser Safari zum Einsatz kommt. Die Firma Google beschreibt eine Reihe von Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

### Expertenmeinung:

Die Schwachstellen sind teils als kritisch zu betrachten. Betroffene Systeme sollten zeitnah gepatcht werden.

## 3.14 Apple iOS CFF Font Parsing and IOSurface Integer Overflow

Risiko: **kritisch**  
 Remote: Ja  
 Datum: 03.08.2010  
 scip DB: <http://www.scip.ch/?vuldb.4156>

iOS (bis Juni 2010 iPhone OS) ist ein mobiles Betriebssystem der Firma Apple. Es basiert auf Mac OS X und ist das Standard-Betriebssystem der Apple-Produkte iPhone, iPod touch und iPad. Es bietet eine Anbindung zu dem iTunes Store und dem App Store. Der Researcher comex 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 kann durchaus kritisch Auswirkungen nach sich ziehen. Betroffene Systeme sollten daher zeitnah gepatcht werden, um eine Kompromittierung zu vermeiden.

## 3.15 Google Chrome verschiedene

## 4. Statistiken Verletzbarkeiten

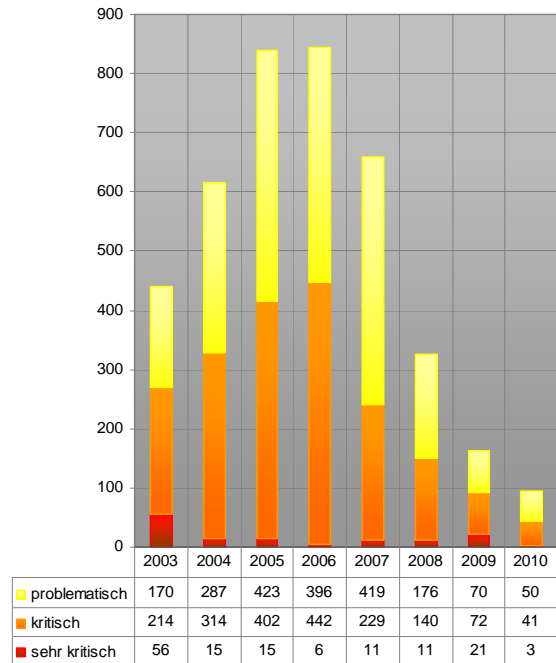
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



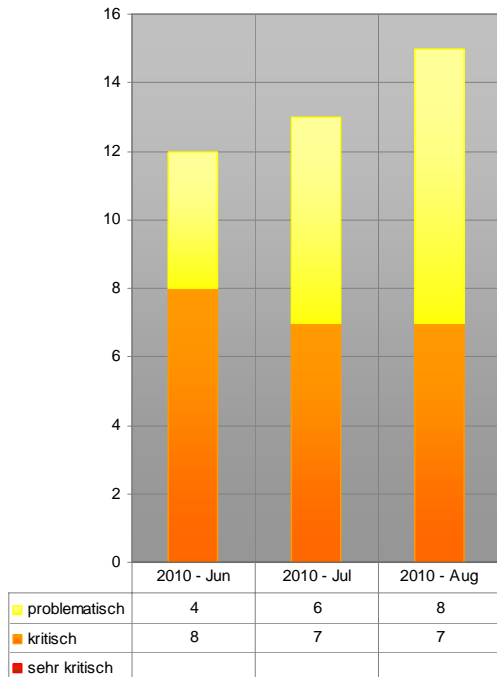
<http://www.scip.ch/?vuldb>

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.

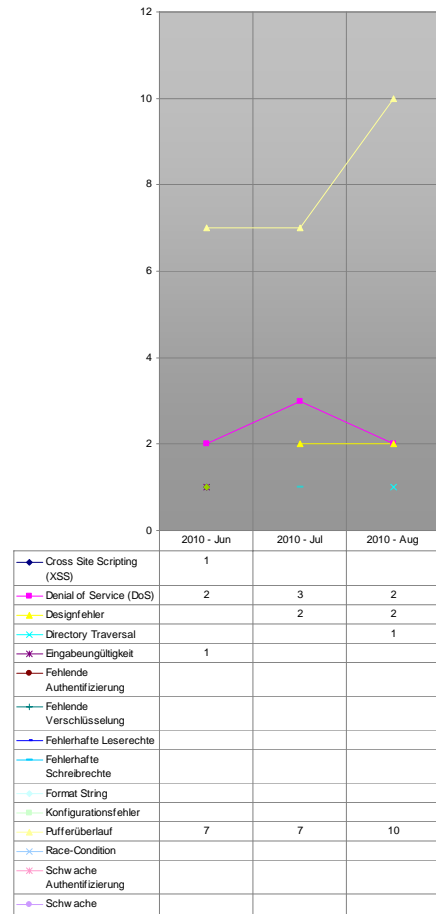
Auswertungsdatum: 19. August 2010



Verlauf der Anzahl Schwachstellen pro Jahr

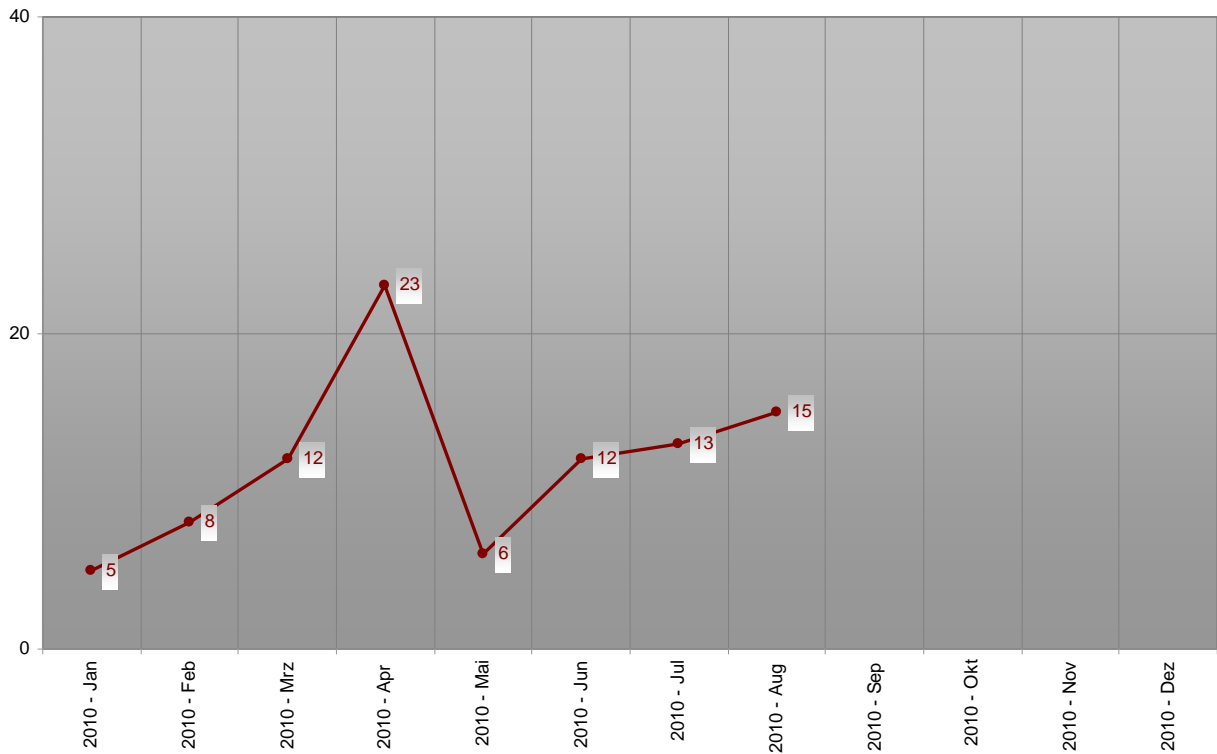


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

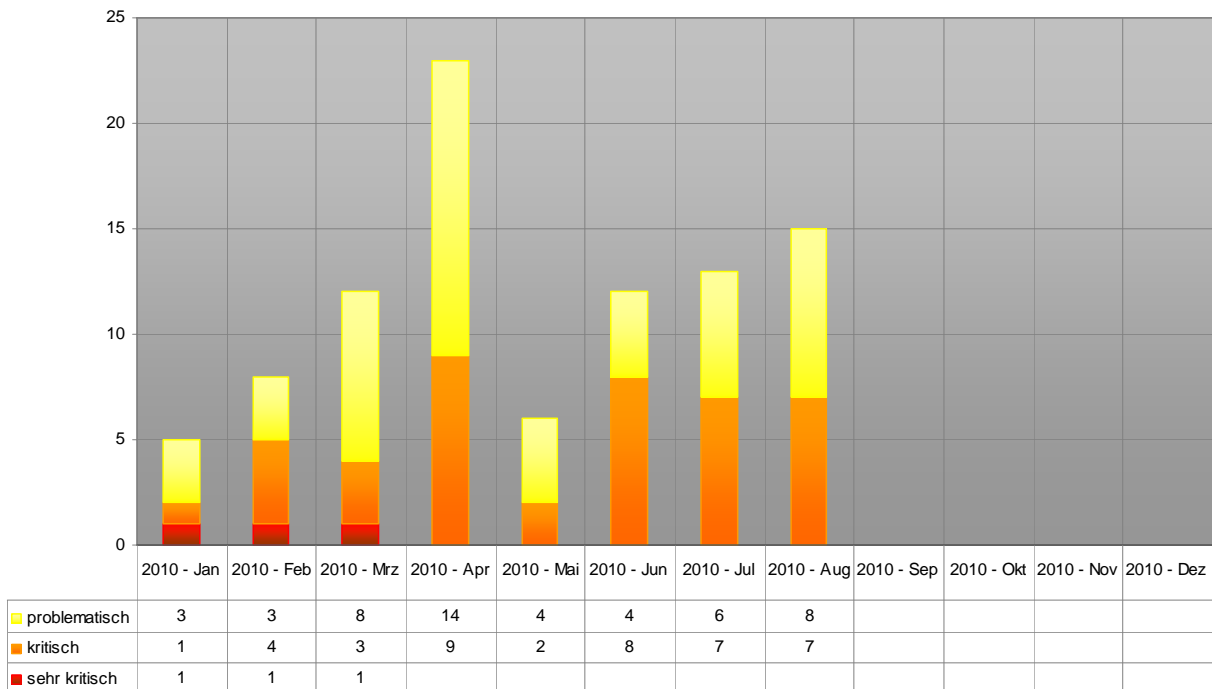


Verlauf der letzten drei Monate Schwachstelle/Kategorie

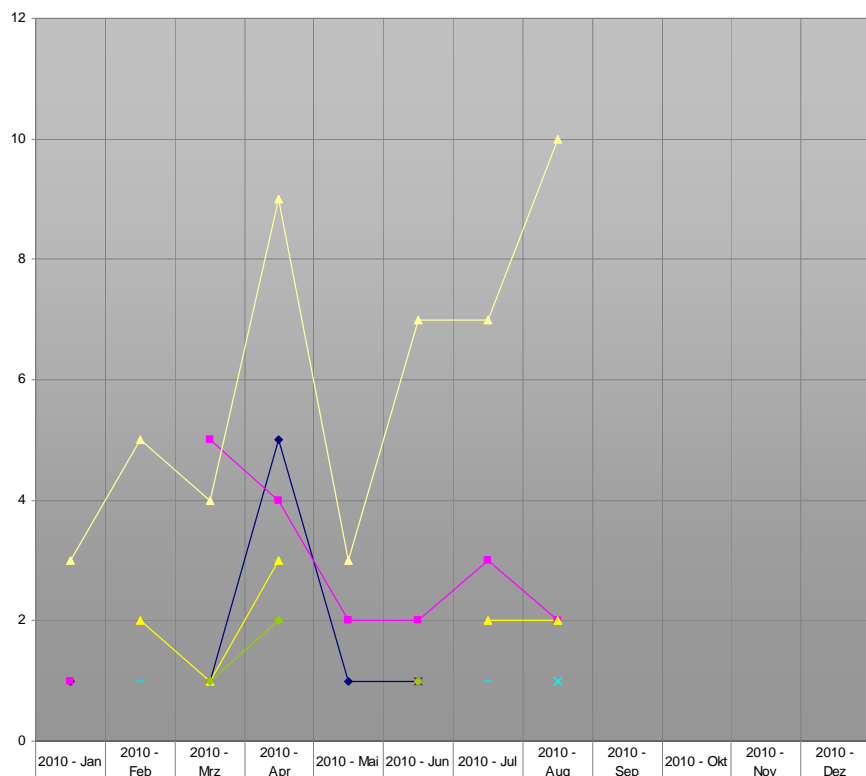
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2010



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2010

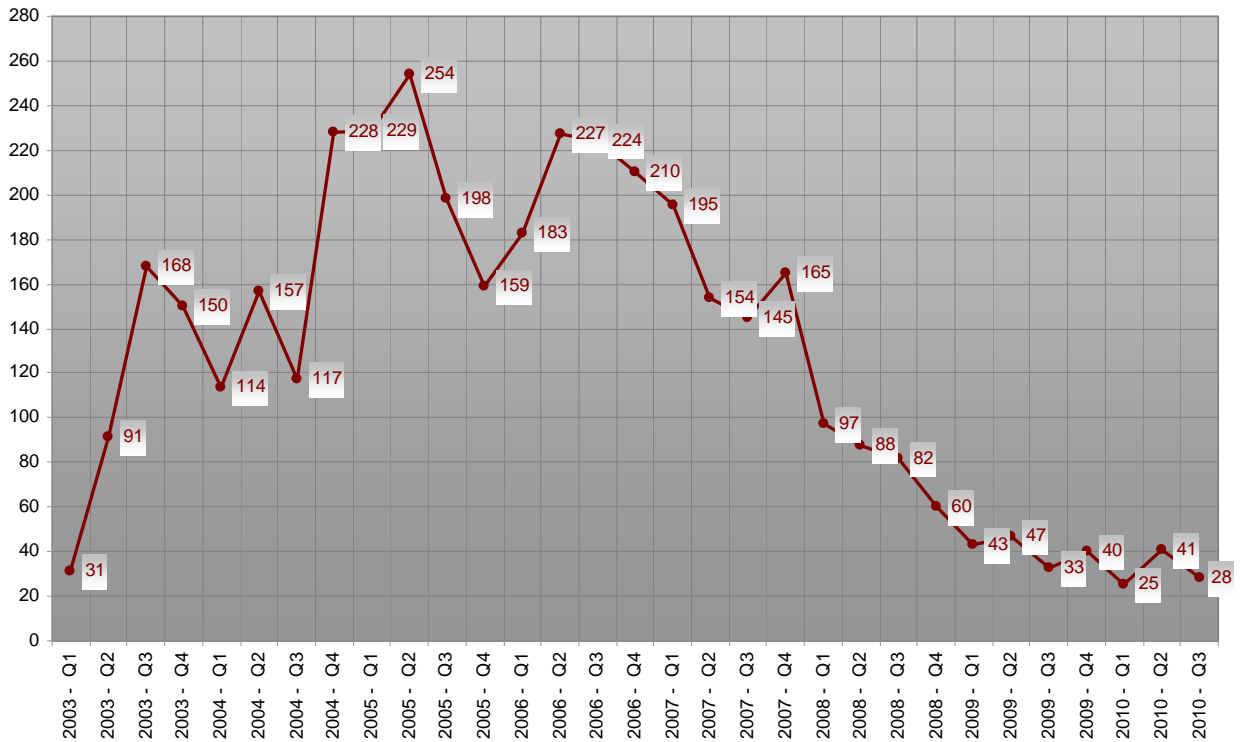


	2010 - Jan	2010 - Feb	2010 - Mrz	2010 - Apr	2010 - Mai	2010 - Jun	2010 - Jul	2010 - Aug	2010 - Sep	2010 - Okt	2010 - Nov	2010 - Dez
◆ Cross Site Scripting (XSS)	1		1	5	1	1						
◆ Denial of Service (DoS)	1		5	4	2	2	3	2				
◆ Designfehler		2	1	3			2	2				
◆ Directory Traversal								1				
◆ Eingabeungültigkeit						1						
◆ Fehlende Authentifizierung												
◆ Fehlende Verschlüsselung												
◆ Fehlerhafte Leserechte												
◆ Fehlerhafte Schreibrechte												
◆ Format String												
◆ Konfigurationsfehler												
◆ Pufferüberlauf	3	5	4	9	3	7	7	10				
◆ Race-Condition												
◆ Schwache Authentifizierung												
◆ Schwache Verschlüsselung												
◆ SQL-Injection												
◆ Symink-Schwachstelle												
◆ Umgehungs-Angriff		1					1					
◆ Unbekannt			1	2		1						

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2010

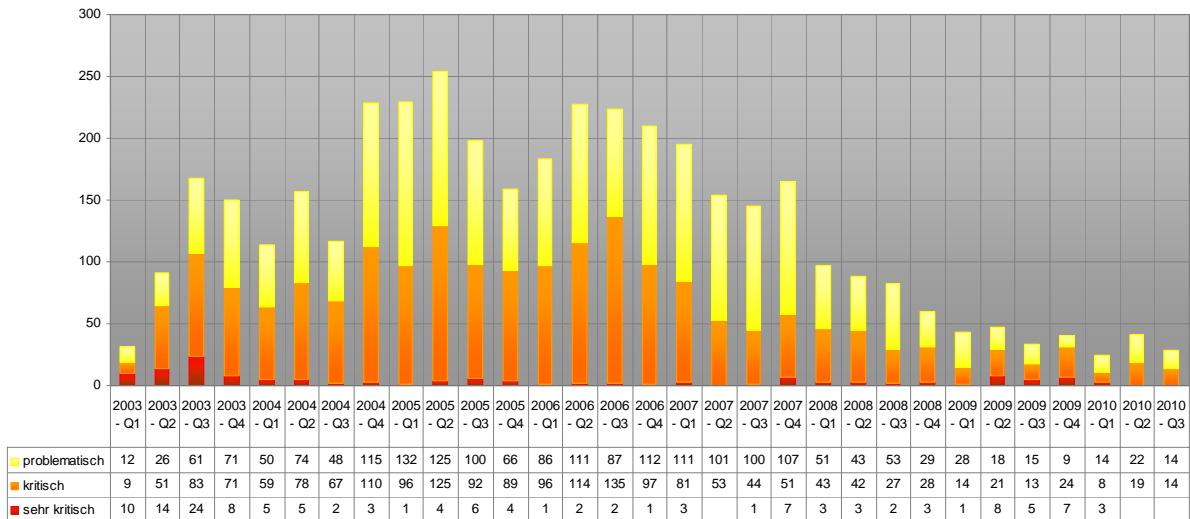


Registrierte Schwachstellen by scip AG



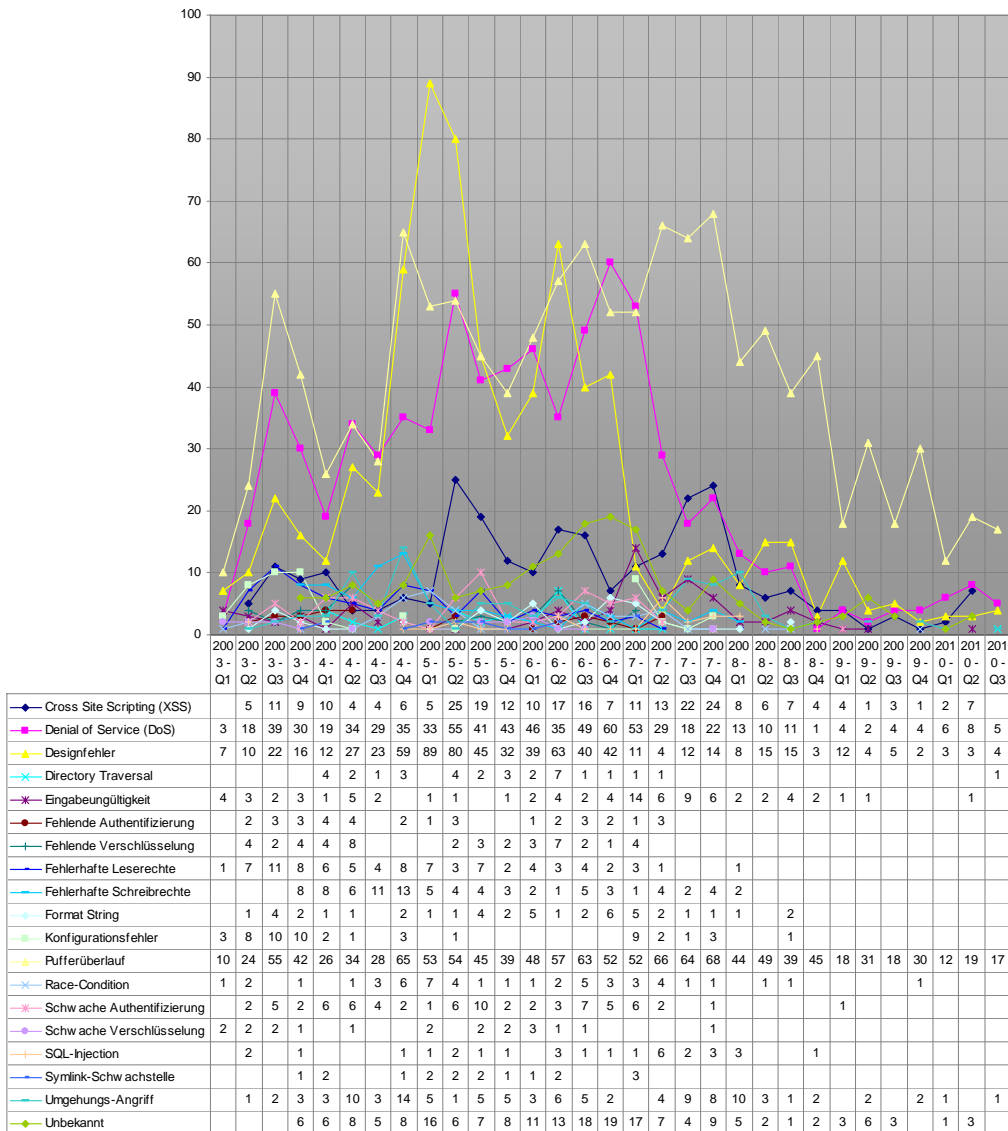
Verlauf der Anzahl Schwachstellen pro Quartal seit 2003 Q1

scip monthly Security Summary 19.08.2010



Verlauf der Anzahl Schwachstellen/Schweregrad pro Quartal seit 2003 Q1





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 HTML5 Cross Origin Request Sicherheit

23.07.2010 Marc Ruef, [maru@scip.ch](mailto:maru@scip.ch)

Die Weiterentwicklung der modernen Informationsgesellschaft schafft stetig neue Anforderungen an das Internet. Als Folge davon werden fortwährend neue Standards geschaffen und bestehende Technologien weiterentwickelt. Als Kernbestandteil des modernen World Wide Web gilt die Seitenbeschreibungssprache HTML. Gegenwärtig wird die Entwicklung von [HTML5](#) vorangetrieben. Populäre Webseiten wie YouTube versuchen das proprietäre Flash durch die neuen Multimedia-Funktionen von HTML5 [abzulösen](#) und verhelfen so früher oder später der neuen Version zum breitflächigen Durchbruch.

Gegenwärtig ist der siebte Arbeitsentwurf herausgegeben worden. Noch nicht alle Webbrowser unterstützen die jeweiligen Spezifikationen. Es ist jedoch absehbar, dass so manches neue Feature schnellstmöglich implementiert werden will, um die Reichhaltigkeit des World Wide Web vorantreiben zu können.

Eine der zentralen Funktionen von HTML5 ist [Cross Origin Request](#) und erweitert die Möglichkeiten des Browsers, Ajax-ähnliche Zugriffe domänenübergreifend durchzuführen. Die traditionelle [Same Origin Policy](#) sah vor, dass mit Javascript umgesetzte HTTP-Anfragen nur für jene Domain umgesetzt werden kann, von der das Javascript-Dokument geladen wurde. Mit COR können nun auch HTTP-Anfragen für gänzlich andere Webseiten durchgeführt werden. Die Vernetzung unterschiedlicher Angebote wird damit vorangetrieben:

Web application technologies commonly apply same-origin restrictions to network requests. These restrictions prevent a (client-side) Web application running from one origin from obtaining data retrieved from another origin, and also limit the amount of unsafe HTTP requests that can be automatically launched toward destinations that differ from the running application's origin.

Vielerorts wird die Sicherheit von COR [reguliert](#). Die Diskussionen fokussieren sich dabei jedoch auf die Sicht der Webentwickler und Webadministratoren. COR-Rückantworten

können durch den Browser nur dann angesteuert werden, wenn der Server in seiner Rückantwort die Header-Zeile [Access-Control-Allow-Origin](#) mitschickt, wobei als Parameter das Quellsystem angegeben werden muss. Beispiel PHP:

```
header('Access-Control-Allow-Origin:
http://www.scip.ch/demo/cor/*');
echo 'This is a successful cor re-
sponse.';
```

Als Hauptrisiko hiervon wird vorgetragen, dass freizügige Zugriffsmöglichkeiten (z.B. mit dem Wildcard-Zeichen \*) zu unerwünschten Datenabfragen führen können.

Unseres Erachtens ist dieses Risiko *im Verhältnis* vernachlässigbar. Die Webapplikation sollte sowieso eine umfassende Prüfung durchführen, ob das Quellsystem den gewünschten Datenzugriff durchführen darf. Authentisierung und Session-Management sind nach wie vor erforderlich und können durch den Access-Control Header nur bedingt ersetzt – stattdessen aber *ergänzt* – werden.

Das grössere Problem von COR ist jedoch die Möglichkeit von Webadministratoren, dass diese Webbrowser zu automatisierten Zugriffen *auf anderen Webseiten* zwingen können. Durch den Besuch einer vermeintlich legitimen Webseite kann ohne Probleme eine [Cross Site Request Forgery](#) durchgesetzt werden. Nachfolgendes Javascript-Snipplet kann in `onload` aufgerufen werden, um automatisch eine weiterführende Anfrage durchzusetzen:

```
function req(){
    var cor;
    if(window.XDomainRequest){
        cor = new XDomainRequest();
        if(cor){
            cor.onload = func-
tion(){
                alert(cor.responseText);
            }
        }else{
            alert('Your Browser does
not support Cross Origin Request');
        }else{
            cor = new XMLHttpRequest();
            cor.onreadystatechange =
function(){
                if(cor.readyState ==
4){
                    alert(cor.responseText);
                }
            }
        }
    }
}
```



```

    cor.open('GET',
'http://www.scip.ch/labs/demos/cor/cor.php');
    cor.send();
}

```

Sieht die aufgerufene Ressource – in diesem Fall <http://www.scip.ch/labs/demos/cor/cor.php> – keinen Zugriff durch die Freigabe über `Access-Control-Allow-Origin` zu, dann kann zwar der Browser nicht auf die in `cor.responseText` vorgesehene Antwort zugreifen. Die Anfrage selbst wird aber in jedem Fall, wird COR denn durch den Browser unterstützt, umgesetzt. Es gibt eine Vielzahl an Angriffsszenarien, die mit diesen Möglichkeiten realisiert werden können (sie betreffen Teilweise auch [SOP](#)):

- **CSRF:** Mit einer Cross Site Request Forgery wird eine Anfrage umgesetzt, die eine Manipulation einer Ressource vorzunehmen in der Lage ist. Zum Beispiel, indem ein Zugriff auf die Datei `/adduser.php?u=attacker&p=1234` einer Webseite vorgenommen wird.
- **Bruteforce:** Mit einer Aneinanderreihung von Anfragen kann eine Bruteforce-Attacke auf eine Ressource vorgenommen werden.
- **Infektion:** Durch den Aufruf unsicherer Skripte lassen sich Infektionen durch Würmer vorantreiben. Diese wird dann nicht mehr durch die infizierten Server selbst initiiert, sondern durch die Besucher der Seiten. Die wahre Quelle einer Infektion wird dadurch schwierig identifizierbar.
- **Flooding:** Wenn eine Vielzahl an Benutzern für Anfragen eingespannt werden, lässt sich eine webbasierte Distributed Denial of Service-Attacke (DDoS) realisieren.
- **Tracking:** Indem ein Pinging im Hintergrund umgesetzt wird, kann das Tracking eines Benutzers im Sinn eines Webbugs realisiert werden (siehe [Facebook Like Button Tracking](#)).
- **Header-Injection:** Durch das Injizieren des jeweiligen Headers besteht die Möglichkeit, die Limitierungen des Browsers zu umgehen. (Danke an [@x3l\\_ch](#))

Wir empfehlen dem HTML5-Gremium, die Legitimität der COR-Zugriffe nicht erst durch die angefragte Ressource bestimmen und *danach* durch den Client anhand der Rückantwort limitieren zu lassen. Stattdessen sollte schon *vor* dem Zugriff eine Einschränkung durchgesetzt werden. Und genau hier täte es eigentlich aus Sicht der

Sicherheit gut, bei der klassischen Same Origin Policy zu bleiben – Stattdessen wird jedoch die Browser-Sicherheit den technischen Möglichkeiten von COR geopfert.

Die Benutzer haben das Nachsehen, sind sie denn in erster Linie auf die Sicherheitsmechanismen der Browserhersteller angewiesen. Es ist zu hoffen, dass die Browserentwickler darum bemüht sind, dass sich *granulare Einstellungen* in der Konfiguration des Webbrowsers vornehmen lassen, um Ressourcen dediziert Sperren oder eine manuelle Freigabe angehen zu können.

## 6. Bilderrätsel

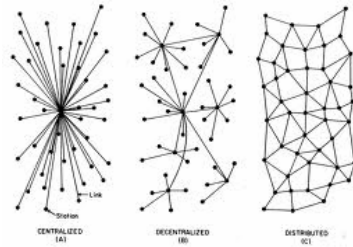


FIG. 1 - Centralized, Decentralized and Distributed Networks



GESUCHTE BEGRIFFE		
		of
11 (english)	6 (english)	7 (english)

LÖSUNGSWORT

### Wettbewerb

Mailen Sie uns das Lösungswort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten.

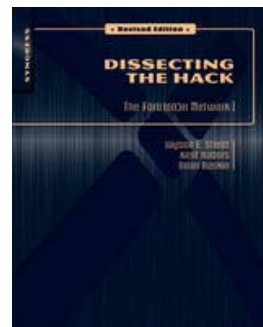
Das Los entscheidet über die Vergabe des Preises. Teilnahmerecht sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.08.2010**.

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.

Gewinnen Sie eines von drei signierten Exemplaren des Buches „Dissecting the Hack: The F0rb1dd3n Network, Revised Edition“ von Jayson E. Street.

*"Welcome to hacker fiction -- like SciFi, but you don't get to make the good stuff up."* – Dan Kaminsky, Recursion Ventures



<http://f0rb1dd3n.com>  
Jayson E. Street, Kent Nabors, Brian Baskin  
360 Seiten, Englisch

## 7. Impressum

Herausgeber:



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 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 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 beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, Trend-Micro, 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 Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)