

Contents

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

1. Editorial

Code from Hell

Irgendwie mag ich Monk, obschon ich bisher nur zwei Folgen partiell gesehen habe. Das Problem ist nicht, dass ich die Serie nicht gut finde. Viel mehr habe ich momentan schon genug zu tun mit den Serien, die ich bisher gucke. Eine meiner liebsten Szenen war, als Monk einen chinesische Verbrecher, dem er noch nichts nachweisen konnte, aufsuchte. Der Chinese machte gerade Klimmzüge und zählte während des etwas verworrenen Verhörs unablässig seine Erfolge: 97, 98, ... Als das Gespräch beendet schien und sich Monk verabschieden wollte, hörte der gute Mann bei 99 auf. Monk ab seiner Obsession sichtlich unruhig nötigte den gut gebauten Herrn, doch die 100 voll zu machen. Das Gespräch ging per Zufall weiter und da war er nun: Der 101ste Klimmzug! Monk kriegte fast einen Herzinfarkt.



Leute mit Zwangsstörungen sind diesbezüglich nicht zu beneiden. Ich kenne genug Leute, die in der Hinsicht tagtäglich zu kämpfen haben. Auch ich muss eingestehen, dass gewisse Dinge in mir eine unendliche Spannung generieren. Früher konnte ich es nicht leiden, wenn ich auf dem Gehweg die Kante einer Steinplatte berühren musste. Also wich ich ihnen aus. Das war eher ein Spiel und wenn ich denn mal in Eile war, war es mir doch eher egal. Zum Glück.

Bei einer der vielen Quelltext-Analysen, die ich in letzter Zeit durchgeführt habe, durfte ich mich mit ASP-Code herumschlagen. Ja, ich mag ASP auch nicht, aber in diesem Fall konnte ich schliesslich nicht auswählen. So machte ich mich dann daran, mir die Banking-Applikation etwas genauer anzuschauen. Ich gehe dabei immer in gleicher systematischer Weise vor: Zuerst einmal die Ausgabefunktion suchen, dann die Eingaben (User-Input) identifizieren und dann den Pfad dazwischen analysieren (z.B. String-Manipulationen, Datenbankzugriffe, etc.).

In meinem Leben habe ich schon die eine oder andere Anwendung geschrieben. Ich bin zwar kein professioneller Entwickler, doch meine ich Programmcode verstehen und optimieren zu können. Ebenso bin ich mir den jeweiligen Code-Konventionen, wie sie bei grösseren Projekten und Firmen eingesetzt werden (z.B. Apache Software Foundation oder dem Linux Kernel) sehr wohl bewusst. Das einheitliche Nutzen von Variablennamen, Auslagerung von Konstanten in bestimmte Bereiche und das Einhalten von Whitespace-Abständen erachte ich als sehr wichtig. Auch wenn der Endanwender nichts davon mitbekommt, haben solche Dinge massgeblichen Einfluss auf die Qualität der Lösung.

Die besagte Quelltext-Analyse sollte den Monk in mir wecken. Da wurde auf eine zentralisierte Ausgabefunktion verzichtet. Gerade bei Webanwendungen, die im Regelfall in höchstem

Masse Interaktion mit nicht-vertrauenswürdigen Benutzern aufweisen, ist das eine Todsünde. Denn so müsste man nun die Eingabeüberprüfung an den jeweiligen Eingabepunkten durchführen. Hat die Anwendung mehrere hundert Textfelder, dürfte der Code in sinnloser Weise anwachsen. Ist der Entwickler halbwegs intelligent, schreibt er sich wenigstens eine einheitliche Funktion, die er öffentlich zugänglich macht. Ist der Entwickler hingegen weniger intelligent, wird er mit Replace-Zugriffen die einzelnen Parameter separat abarbeiten. Letzteres war hier der Fall (der Aufwand der Prüfung steigt dabei für mich exponentiell an!).

Als ich die Codebasis so durchforstete wollte ich fortwährend die Variablennamen anpassen, die kaputten while-Schleifen optimieren und unnötige bool'sche Verknüpfungen in if-Entscheidungen aufheben. Es zuckte in meinen Fingern, den Code so zu optimieren, dass er sowohl lesbar als auch halbwegs effizient ausführbar wurde. Doch leider werde ich nicht dafür bezahlt. So musste ich halt damit Vorlieb nehmen, eine architektonisch und entwicklungstechnisch wirklich schlimme Anwendung durchwühlen zu müssen.

In solchen Fällen habe ich es mir zur Gewohnheit gemacht, im Abschlussbericht auch auf derlei Mängel hinzuweisen. Auf den ersten Blick scheint es kein "Security Issue" zu sein, wenn man zum Beispiel komplexere if-Strukturen anstelle von case-Blöcken verwendet. Doch längerfristig wird unter Umständen die Wartung des Codes in derartiger Weise erschwert, dass das ungewollte Einführen von Schwachstellen statistisch nicht mehr von der Hand zu weisen ist. Manche Entwickler fühlen sich sonst schon angegriffen, wenn man sie zu einer Source Code Analyse drängt. Und hat man dann auch noch den allgemeinen Programmierstil zu bemängeln, dann schafft man sich damit keine Freunde. Doch leider ist es nicht meine Aufgabe, mir Freunde zu schaffen. Meine manchmal etwas undankbare Arbeit ist es, Schwachstellen aufzudecken und diese zusammen mit dem Kunden anzugehen, um die Sicherheit einer Lösung bestmöglich verbessern zu können.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 6. Oktober 2008

2. scip AG Informationen

2.1 Web Application Penetration Test

Die Welt ohne Internet und ohne Webseiten ist nicht mehr vorstellbar. Keine Firma ohne Webaufritt! Die Ausprägung beginnt bei einfachen „Visitenkarten im Netz“ über interaktive Firmenvorstellungen mit notwendiger Softwareinstallation im Client-Browser bis hin zu komplexen Webapplikationen mit Datenbankbindung wie E-Banking oder Online-Shops. Alle Personen mit Zugang zum Internet haben somit Zugriff auf die so bereitgestellten Daten.

Die Herausforderung beginnt nun damit, dass übliche Sicherheitsmassnahmen wie Firewalls oder Antiviren Lösungen nicht den notwendigen Schutz bieten können. Erschwerend kommt dazu, dass Software von Menschen programmiert wird und selten ohne Fehl und Tadel ist.

Die Grosse Frage lautet nun: wie kann ich meinen Kunden, Interessenten und Partner Zugriff auf meine Webseite und Dienste gewähren ohne, dass ich oder meine Dienstanwender und Webseitenbenutzer befürchten müssen Opfer von zum Beispiel einfachem Vandalismus, Erpressung, Datendiebstahl oder Informationsmanipulation zu werden?

Diese Fragestellung lässt sich durch Webapplication Penetration Tests beantworten. Nach der Definierung der Risikoklassifizierung und den zu erwartenden Angreifertypen werden zielgerichtete, kundenbasierende und lösungsorientierte Testreihen umgesetzt um die Sicherheit Ihrer Webangebote zu determinieren, detaillierte Gegenmassnahmen zu planen und die definierte Sicherheit Ihrer Werte langfristig zu sichern.

Dank unserer langjährigen Erfahrung in diesem spezifischen Gebiet inklusive der Programmierung eigener Penetration Test Software und unserem ausgewiesenen Expertenwissen haben wir als scip AG die Ehre die unterschiedlichsten Webapplikationen (E-Banking, Online-Shop etc.) vieler namhafter nationaler- und internationaler Unternehmungen überprüft zu haben und dabei geholfen haben diese abzusichern.

Zählen auch Sie auf uns!

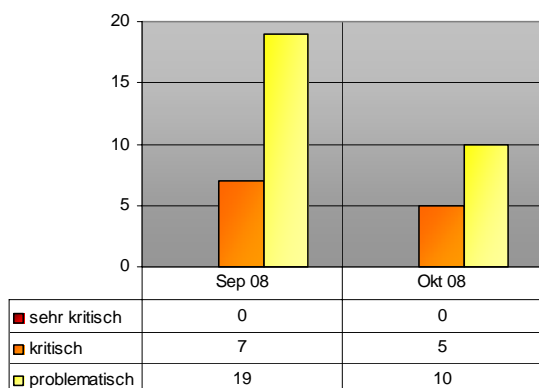
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.



Die Dienstleistungspakete [\)scip/ pallas](#) liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind.



Contents:

- 3854 VLC Player Pufferüberlauf bei Verarbeitung von XSPF Dateien
- 3853 Microsoft Windows Ancillary Function Driver Codeausführung
- 3852 Microsoft Windows SMB Buffer Underflow
- 3851 Microsoft Windows IIS IPP Service Integer Overflow
- 3850 Microsoft Windows Doppelte Speicherfreigabe führt zu Privilege Escalation
- 3849 Microsoft Windows Fehler in Eingabeverarbeitung führt zu Privilege Escalation
- 3846 Microsoft Windows Fenstereigenschaften (Privilege Escalation)
- 3845 Microsoft Windows Active Directory Pufferüberlauf
- 3842 Microsoft Excel unzureichende Datenvalidation in VBA Performance Cache
- 3840 Adobe Flash Player "Clickjacking" Schwachstelle
- 3839 mIRC "PRIVMSG" Pufferüberlauf
- 3838 Citrix Presentation Server Privilege Escalation
- 3836 phpMyAdmin PMA_escapeJsString() Cross-Site Scripting
- 3835 phpMyAdmin "sort_by" PHP Codeausführung

3.1 VLC Player Pufferüberlauf bei Verarbeitung von XSPF Dateien

Einstufung: **problematisch**
 Remote: Ja
 Datum: 16.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3854>

VideoLAN ist der Name eines Projekts der französischen Ingenieurschule École Centrale Paris aus Châtenay-Malabry bei Paris. In Zusammenarbeit mit unabhängigen Entwicklern aus über 20 Ländern und ehemaligen Studenten der Schule entwickelt VideoLAN eine quelloffene Streaming-Lösung für digitale Audio- und Videoformate. Das Projekt hat über 50 Mitglieder, von denen etwa 15 bis 20 regelmäßig mitarbeiten. Das berühmteste Mitglied des Teams ist der norwegische Programmierer Jon Lech Johansen, der durch die Umgehung des Kopierschutzes CSS von DVDs und des im iTunes Music Store benutzten DRM-Systems FairPlay auch in den Massenmedien bekannt wurde. Francisco Falcon von Core Security fand eine Schwachstelle bei der Verarbeitung von XSPF Datentypen durch den beliebten Player. Durch einen Vorzeichenfehler in der Funktion `parse_track_node()` kann dadurch ein Pufferüberlauf provoziert werden, der zur Ausführung beliebigen Codes missbraucht werden kann.

Expertenmeinung:

VLC ist nach wie vor (zurecht) einer der populärsten Player für verschiedenste Dateiformate. Dass sich das Dasein als Tausendsassa nicht immer von seiner sonnigen Seite zeigt, beweist die vorliegende Lücke mit Erfolg. Nutzer der populären Applikation sollten XSPF Datentypen bis auf weiteres mit Argwohn betrachten und alsbald möglich einen in Kürze erscheinenden Patch einspielen.

3.2 Microsoft Windows Ancillary Function Driver Codeausführung

Einstufung: **problematisch**
 Remote: Ja
 Datum: 15.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3853>

Microsoft Windows ist ein Markenname für Betriebssysteme der Firma Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie zum Beispiel auch GEM oder PC/GEOS), inzwischen hat Microsoft das DOS-Fundament aber völlig aufgegeben und setzt

ausschließlich auf Windows-NT-Betriebssystemversionen. Wie Fabien Le Mentec in einem Advisory festhält existiert eine Schwachstelle im Ancillary Function Driver. Hier werden Speicherbereiche vor deren Ausführung nicht ausreichend geprüft und können daher zur Ausführung beliebigen Codes im Kernel Mode missbraucht werden.

Expertenmeinung:

Auch diese Schwachstelle reiht sich bedauerlicherweise nahezu nahtlos in die Reihe von Schwachstellen in diversen Windowsversionen diesen Monats ein. Auch hier sei empfohlen, so bald wie möglich die notwendigen Patches einzuspielen, um diese Lücken zu schliessen.

3.3 Microsoft Windows SMB Buffer Underflow

Einstufung: **problematisch**
 Remote: Ja
 Datum: 14.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3852>

Microsoft Windows ist ein Markenname für Betriebssysteme der Firma Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie zum Beispiel auch GEM oder PC/GEOS), inzwischen hat Microsoft das DOS-Fundament aber völlig aufgegeben und setzt ausschließlich auf Windows-NT-Betriebssystemversionen. Durch einen Fehler von Dateinamen über Microsofts proprietäres SMB Protokoll kann ein Buffer Underflow provoziert werden, der zur Ausführung beliebigen Codes missbraucht werden kann.

Expertenmeinung:

Auch diese Schwachstelle reiht sich bedauerlicherweise nahezu nahtlos in die Reihe von Schwachstellen in diversen Windowsversionen diesen Monats ein. Auch hier sei empfohlen, so bald wie möglich die notwendigen Patches einzuspielen, um diese Lücken zu schliessen.

3.4 Microsoft Windows IIS IPP Service Integer Overflow

Einstufung: **problematisch**
 Remote: Ja
 Datum: 14.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3851>

Microsoft Windows ist ein Markenname für

Betriebssysteme der Firma Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie zum Beispiel auch GEM oder PC/GEOS), inzwischen hat Microsoft das DOS-Fundament aber völlig aufgegeben und setzt ausschließlich auf Windows-NT-Betriebssystemversionen. Durch einen Fehler in der Implementierung des Internet Printing Protocols kann über einen manipulierten Request ein Integer Overflow provoziert und beliebiger Code zur Ausführung gebracht werden.

Expertenmeinung:

Auch diese Schwachstelle reiht sich bedauerlicherweise nahezu nahtlos in die Reihe von Schwachstellen in diversen Windowsversionen diesen Monats ein. Auch hier sei empfohlen, so bald wie möglich die notwendigen Patches einzuspielen, um diese Lücken zu schliessen.

3.5 Microsoft Windows Doppelte Speicherfreigabe führt zu Privilege Escalation

Einstufung: **kritisch**
 Remote: Ja
 Datum: 14.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3850>

Microsoft Windows ist ein Markenname für Betriebssysteme der Firma Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie zum Beispiel auch GEM oder PC/GEOS), inzwischen hat Microsoft das DOS-Fundament aber völlig aufgegeben und setzt ausschließlich auf Windows-NT-Betriebssystemversionen. Durch eine doppelte Speicherfreigabe bei Multi-Threading Prozessen kann ein Pufferüberlauf ausgelöst werden, der zur Ausführung beliebigen Programmcodes ausgenutzt werden kann.

Expertenmeinung:

Gleich drei kritische Schwachstellen hat Microsoft diesen Monat im Bereich seiner Core-Produkte (Windows 2003 Server / Windows XP) zu beklagen. Die hier aufgeführten Schwachstellen sind abschliessend als kritisch einzustufen und sollten daher baldmöglichst durch das Einspielen entsprechender Patches adressiert werden.

3.6 Microsoft Windows Fehler in Eingabeverarbeitung führt zu

Privilege Escalation

Einstufung: **kritisch**
Remote: Ja
Datum: 14.10.2008
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3849>

Microsoft Windows ist ein Markenname für Betriebssysteme der Firma Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie zum Beispiel auch GEM oder PC/GEOS), inzwischen hat Microsoft das DOS-Fundament aber völlig aufgegeben und setzt ausschließlich auf Windows-NT-Betriebssystemversionen. Wie Microsoft unlängst in einem Advisory publizierte, existiert eine Schwachstelle bei der Verarbeitung gewisser User-Mode Eingabewerte, die zu einem Pufferüberlauf führen und die Ausführung beliebigen Programmcodes erlauben können.

Expertenmeinung:

Gleich drei kritische Schwachstellen hat Microsoft diesen Monat im Bereich seiner Core-Produkte (Windows 2003 Server / Windows XP) zu beklagen. Die hier aufgeführten Schwachstellen sind abschliessend als kritisch einzustufen und sollten daher baldmöglichst durch das Einspielen entsprechender Patches adressiert werden.

3.7 Microsoft Windows Fenstereigenschaften (Privilege Escalation)

Einstufung: **kritisch**
Remote: Ja
Datum: 14.10.2008
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3846>

Microsoft Windows ist ein Markenname für Betriebssysteme der Firma Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie zum Beispiel auch GEM oder PC/GEOS), inzwischen hat Microsoft das DOS-Fundament aber völlig aufgegeben und setzt ausschließlich auf Windows-NT-Betriebssystemversionen. Durch einen Fehler bei der Verarbeitung von Fenstereigenschaften beim Erstellen von Kindprozessen kann ein Pufferüberlauf provoziert werden, durch den beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:

Gleich drei kritische Schwachstellen hat

Microsoft diesen Monat im Bereich seiner Core-Produkte (Windows 2003 Server / Windows XP) zu beklagen. Die hier aufgeführten Schwachstellen sind abschliessend als kritisch einzustufen und sollten daher baldmöglichst durch das Einspielen entsprechender Patches adressiert werden.

3.8 Microsoft Windows Active Directory Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 15.10.2008
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3845>

Der Verzeichnisdienst von Microsoft Windows 2000/Windows Server 2003 heisst Active Directory (AD). Ab der aktuellen Version Windows Server 2008 wird die Kernkomponente als Active Directory Domain Services (ADDS) bezeichnet. Bei einem Verzeichnis (englisch: directory) handelt es sich um eine Zuordnungsliste wie zum Beispiel bei einem Telefonbuch, das Telefonnummern den jeweiligen Anschlüssen (Besitzern) zuordnet. Active Directory ermöglicht es, ein Netzwerk entsprechend der realen Struktur des Unternehmens oder seiner räumlichen Verteilung zu gliedern. Dazu verwaltet es verschiedene Objekte in einem Netzwerk wie beispielsweise Benutzer, Gruppen, Computer, Server, Dateifreigaben und andere Geräte wie Drucker und Scanner und deren Eigenschaften. Mit Hilfe von Active Directory kann ein Administrator die Informationen der Objekte organisieren, bereitstellen und überwachen. Den Benutzern des Netzwerkes können Zugriffsbeschränkungen erteilt werden. So darf zum Beispiel nicht jeder Benutzer jede Datei ansehen oder jeden Drucker verwenden. In der Windows 2000 Version des ActiveDirectory existiert eine Schwachstelle bei der Verarbeitung von LDAP und LDAPS Anfragen. Hier kann ein Pufferüberlauf provoziert werden, der die Ausführung beliebigen Codes erlaubt.

Expertenmeinung:

Die vorliegende Schwachstelle betrifft ausschliesslich Windows 2000, was sie als etwas unkritischer erscheinen lässt. Dennoch sollten Administratoren um eine schnelle Lösung mittels des bereits freigegebenen Patches seitens Microsofts bemüht sein.

3.9 Microsoft Excel unzureichende Datenvalidierung in VBA Performance Cache

Einstufung: **problematisch**
 Remote: Ja
 Datum: 14.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3842>

Microsoft Excel ist ein Tabellenkalkulationsprogramm. Es ist heute die meistverbreitete Software für Tabellenkalkulation. 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 aktuell verfügbare Version ist für Windows Microsoft Excel 2007 (seit 30. November 2006 für Firmenkunden bzw. seit 30. Januar 2007 für Privatkunden) sowie für Mac OS Microsoft Excel 2008 (seit Januar 2008). Durch eine unzureichende Eingabevalidierung von Daten im VBA Performance Cache kann ein Angreifer beliebigen Code durch ein manipuliertes File zur Ausführung bringen.

Expertenmeinung:

Gleich drei Schwachstelle gilt es für Anwender von Microsofts populärer Tabellenkalkulation diesen Monat zu patchen. Es empfiehlt sich an dieser Stelle, die freigegebenen Updates zeitnah einzuspielen, um unnötige Exponierungen zu vermeiden.

3.10 Adobe Flash Player "Clickjacking" Schwachstelle

Einstufung: **problematisch**
 Remote: Ja
 Datum: 08.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3840>

Adobe Flash (kurz Flash, ehemals Macromedia Flash ist eine proprietäre integrierte Entwicklungsumgebung zur Erstellung multimedialer Inhalte, der Flash-Filme. Die resultierenden Dateien liegen im SWF-Format vor, einem auf Vektorgrafiken basierenden Grafik- und Animationsformat. Das Kürzel SWF steht dabei für Shockwave Flash (nicht für "small web format", wie häufig fälschlich angenommen). In aktuellen Versionen kann ein Angreifer sein Opfer dazu bringen, Mikrofon und Webcam für eine Flash Applikation freizugeben, in dem er ihm vorgaukelt dass es sich dabei um normale, für das Laufen der Applikation notwendige, Kontrollelemente handelt. Dadurch erlangt der Angreifer erweiterte Rechte im Player des

Opfers.

Expertenmeinung:

Clickjacking hat sich über die letzten Wochen zum neuen Modewort gemausert und ist auch bei aller Bescheidenheit sicherlich nicht zu unterschätzen. Dennoch ist die professionelle Ausnutzungsrate derzeit noch relativ gering. Es sollte daher ruhig Blut bewahrt werden, um den Patch von Adobe binnen nützlicher Frist einzuspielen und das Problem zu eliminieren.

3.11 mIRC "PRIVMSG" Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 03.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3839>

mIRC wurde vom jordanischen Softwareentwickler Khaled Mardam-Bey entwickelt und am 28. Februar 1995 zum ersten Mal in der Version 2.1a veröffentlicht. Es ist seitdem zu einem der beliebtesten IRC-Clients für Windows gewachsen. Seine Vielseitigkeit beruht hauptsächlich auf der integrierten Scriptsprache mIRC Script, abgekürzt MSL (mIRC Scripting Language). Diese ist so umfangreich, dass mit ihrer Hilfe bereits MP3-Player, IRC-Spiele, HTTP-Server und -Clients sowie DCC-Dateiserver und IRC-Bots implementiert wurden. Um das Schreiben von Programmen in mIRC Script hat sich im IRC eine Gemeinschaft von Anhängern gebildet. "securfrog" publizierte unlängst eine Schwachstelle auf dem hinlänglich populären Portal milw0rm, die bewies dass mIRC durch einen Fehler bei der Verarbeitung von PRIVMSG Befehlen anfällig für einen stackbasierten Pufferüberlauf war. Dadurch kann mittels eines bösartigen IRC Servers beliebiger Code zur Ausführung gebracht werden.

Expertenmeinung:

mIRC ist immer noch eine Standardapplikation im Enduserbereich und somit ist diese Schwachstelle durchaus interessant. So wird mIRC bei Installation auch als Default-Handler für Verknüpfungen in der Form `irc://server.name/channelname` eingerichtet, was eine einfachere Ausnutzbarkeit darstellt. Benutzer sollten reagieren, in dem Sie baldmöglichst auf eine aktualisierte Version umsteigen.

3.12 Citrix Presentation Server Privilege Escalation

Einstufung: **problematisch**

Remote: Ja
 Datum: 01.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3838>

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CTXS gehandelt. Im Geschäftsjahr 2003 hat Citrix einen Umsatz von 588,6 Millionen US-Dollar erwirtschaftet. Im Jahr 2004 erreichte Citrix einen Umsatz von 741 Mio. US-Dollar. 2005 konnte der Umsatz auf 908 Mio. US-Dollar gesteigert werden. In einem Advisory, das Citrix unlängst veröffentlichte, wird eine Privilege Escalation Schwachstelle angedeutet, die aber nicht näher ausgeführt wird. Durch das Ausnutzen dieser Lücke soll es einem Angreifer möglich sein, seine Rechte auf dem Zielsystem auszuweiten, was eine mögliche Kompromittierung nahe legt.

Expertenmeinung:

Auch wenn diese Schwachstelle leider nicht genau spezifiziert wird, so ist eine Privilege Escalation im Citrix Umfeld nicht unbedingt das, was als wünschenswert zu betrachten wäre. Dementsprechend sollte auf diese Lücke unmittelbar mit dem Einspielen des erschienenen Hotfixes reagiert werden, um weitere Auswirkungen zu vermeiden.

3.13 phpMyAdmin PMA_escapeJsString() Cross-Site Scripting

Einstufung: **problematisch**
 Remote: Ja
 Datum: 23.09.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3836>

phpMyAdmin ist eine freie PHP-Applikation zur Administration von MySQL-Datenbanken. Die Administration erfolgt über HTTP mit einem Browser. Daher können auch Datenbanken auf fremden Rechnern über eine Netzwerkverbindung oder über das Internet administriert werden. Für die Nutzung des Programms sind keine Kenntnisse in SQL notwendig, da die Applikation nach dem WYSIWYG-Verfahren arbeitet. Gemäss eines Advisories von Masako Oono existiert ein Fehler in der Library-Funktion PMA_escapeJsString(), die zur Bereinigung von Zeichenketten genutzt wird. Durch den Fehler wird es möglich, beliebigen Inhalt im Kontext der Zielapplikation zur Ausführung zu bringen.

Expertenmeinung:

Und noch eine Schwachstelle in phpMyAdmin: Auch hier gilt die Empfehlung der vorhergehenden Lücke: Als bald möglich sollte ein Update auf die aktuellste Version angestrebt werden.

3.14 phpMyAdmin "sort_by" PHP Codeausführung

Einstufung: **problematisch**
 Remote: Ja
 Datum: 22.09.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3835>

phpMyAdmin ist eine freie PHP-Applikation zur Administration von MySQL-Datenbanken. Die Administration erfolgt über HTTP mit einem Browser. Daher können auch Datenbanken auf fremden Rechnern über eine Netzwerkverbindung oder über das Internet administriert werden. Für die Nutzung des Programms sind keine Kenntnisse in SQL notwendig, da die Applikation nach dem WYSIWYG-Verfahren arbeitet. Norman Hippert identifizierte eine Schwachstelle in aktuellen Versionen der Applikation, bei der Eingaben an den Parameter sort_of nicht korrekt verarbeitet wurden, was die beliebige Ausführung von PHP Code begünstigte.

Expertenmeinung:

Die Kritikalität von Code Execution Schwachstellen in PHP Applikation ist abhängig von der jeweiligen Konfiguration des Hostsystems. Im Fall der vorliegenden Schwachstelle empfiehlt sich, so oder so, die umgehende Einspielung des aktuellen Updates um diese Schwachstelle zu schliessen.

4. Statistiken Verletzbarkeiten

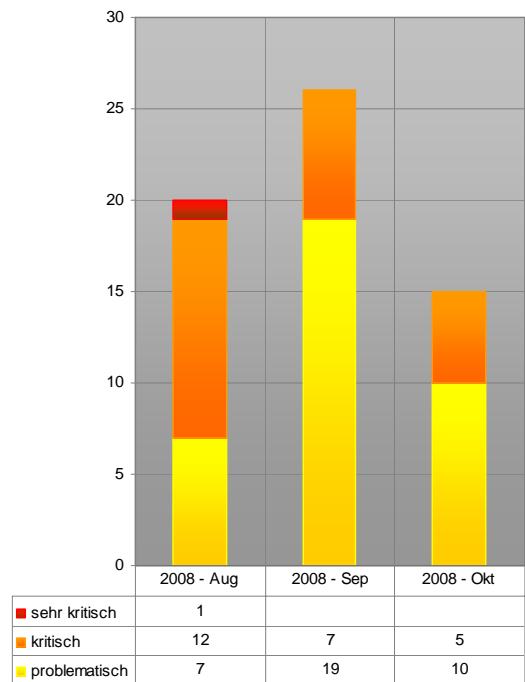
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



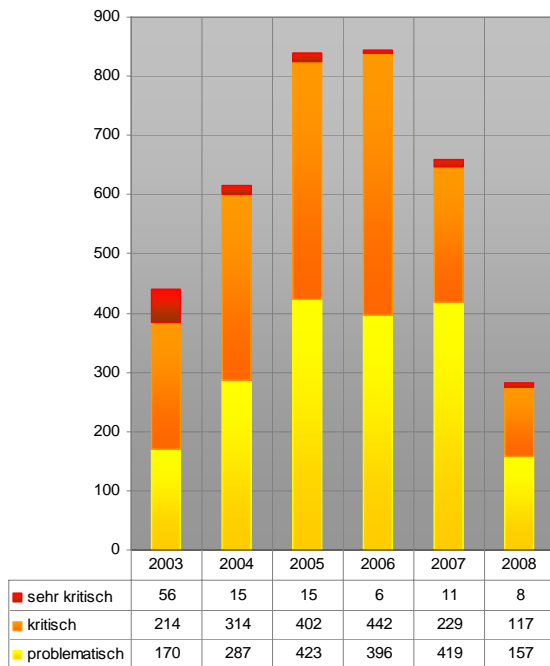
<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

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

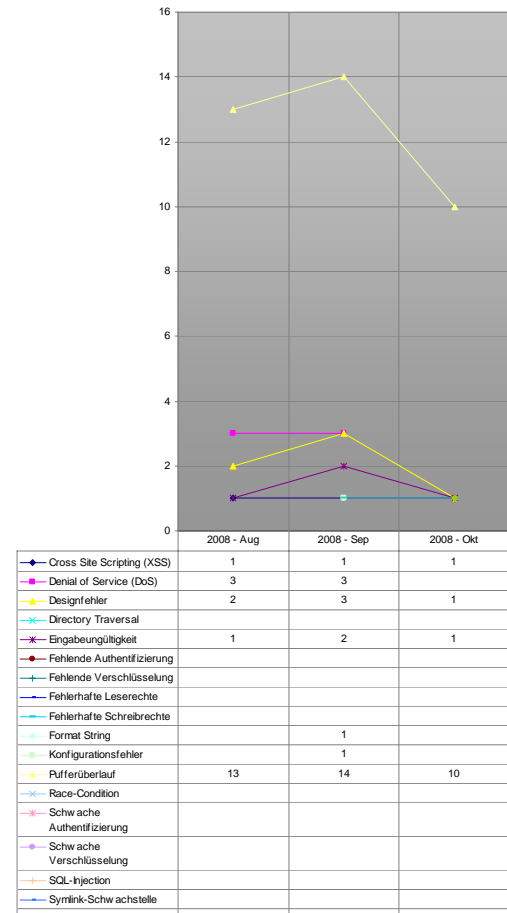
Auswertungsdatum: 19. Oktober 2008



Verlauf der Anzahl Schwachstellen pro Jahr

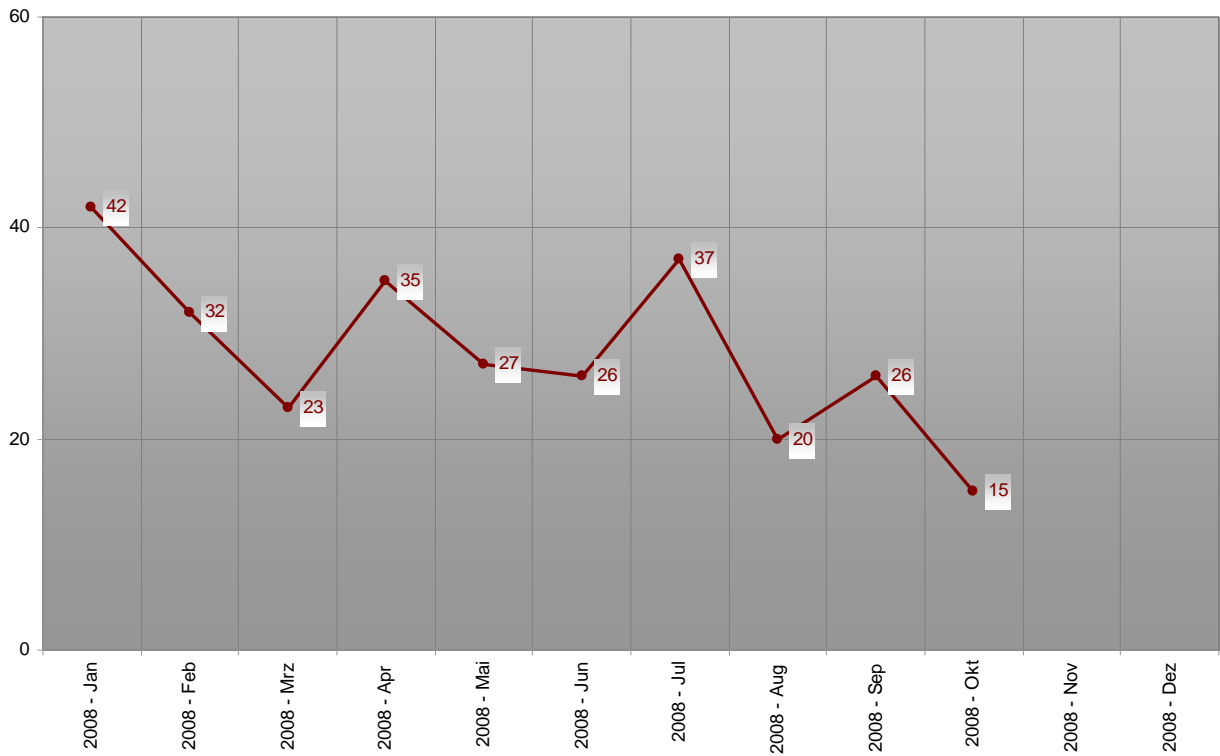


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

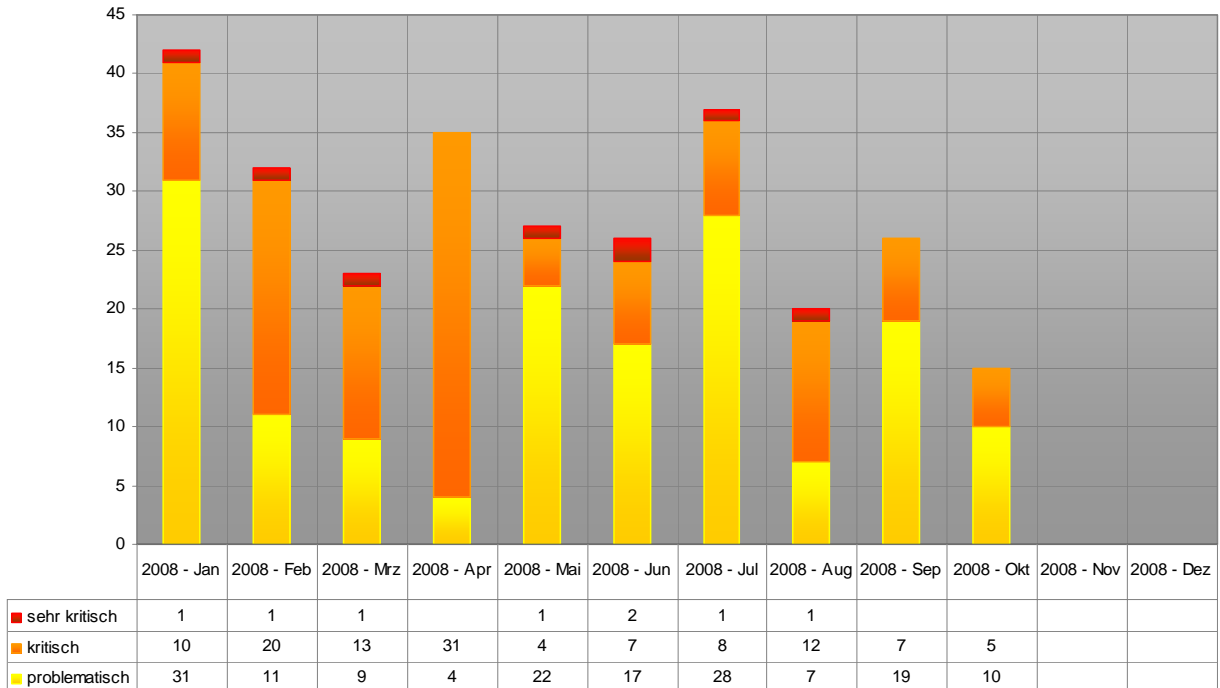


Verlauf der letzten drei Monate Schwachstelle/Kategorie

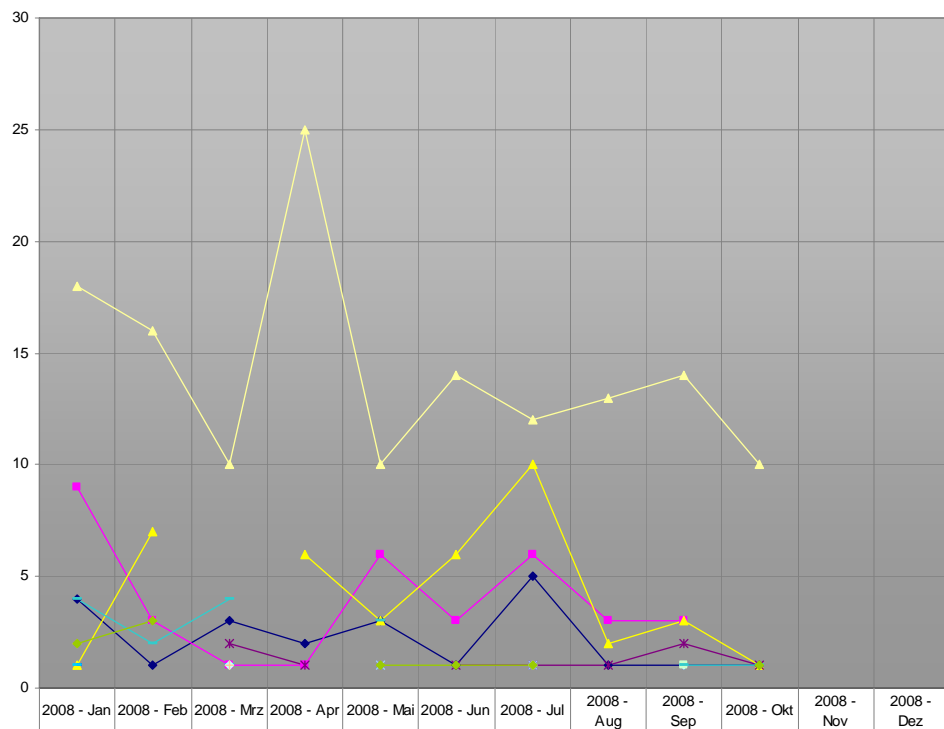
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008



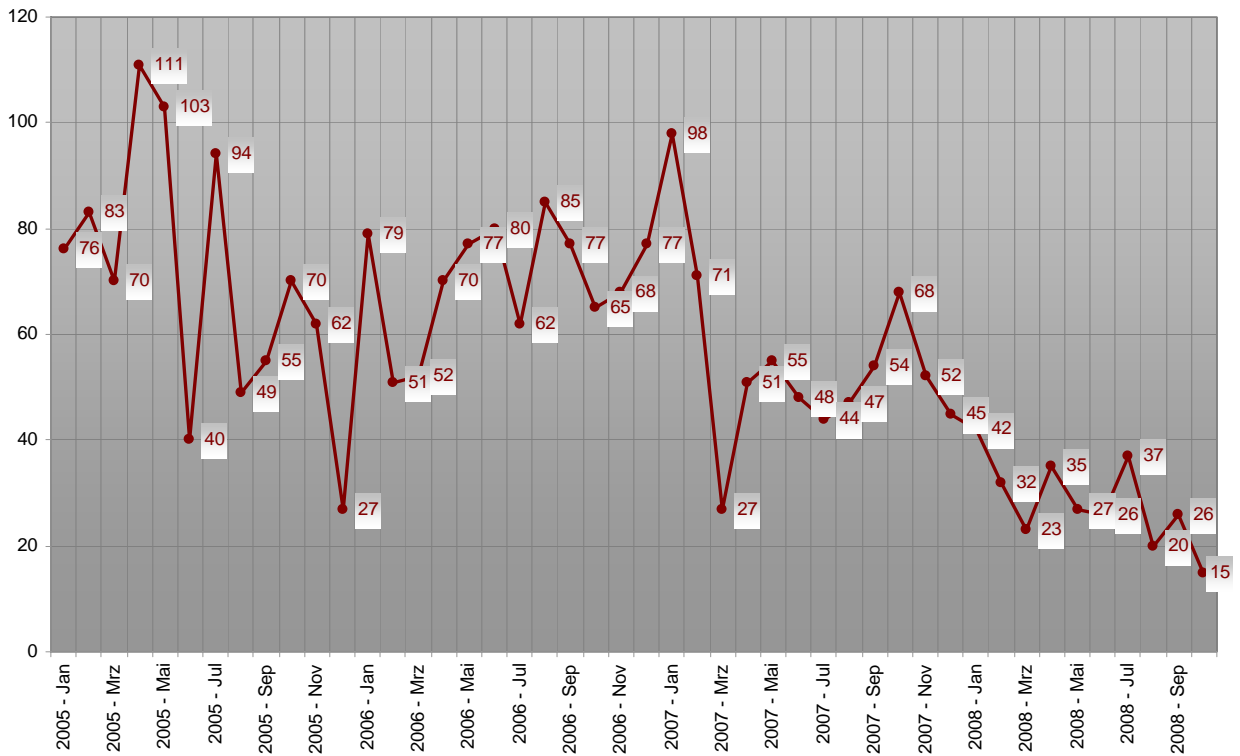
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2008



	2008 - Jan	2008 - Feb	2008 - Mrz	2008 - Apr	2008 - Mai	2008 - Jun	2008 - Jul	2008 - Aug	2008 - Sep	2008 - Okt	2008 - Nov	2008 - Dez
◆ Cross Site Scripting (XSS)	4	1	3	2	3	1	5	1	1	1		
■ Denial of Service (DoS)	9	3	1	1	6	3	6	3	3			
▲ Designfehler	1	7		6	3	6	10	2	3	1		
✕ Directory Traversal												
✖ Eingabeungültigkeit			2	1		1	1	1	2	1		
● Fehlende Authentifizierung												
└─ Fehlende Verschlüsselung												
─ Fehlerhafte Leserechte	1											
─ Fehlerhafte Schreibrechte	1		1									
○ Format String			1				1		1			
■ Konfigurationsfehler									1			
▲ Pufferüberlauf	18	16	10	25	10	14	12	13	14	10		
✕ Race-Condition					1		1					
✖ Schwache Authentifizierung												
○ Schwache Verschlüsselung												
─ SQL-Injection	2		1									
─ Symlink-Schwachstelle												
─ Umgehungs-Angriff	4	2	4		3				1	1		

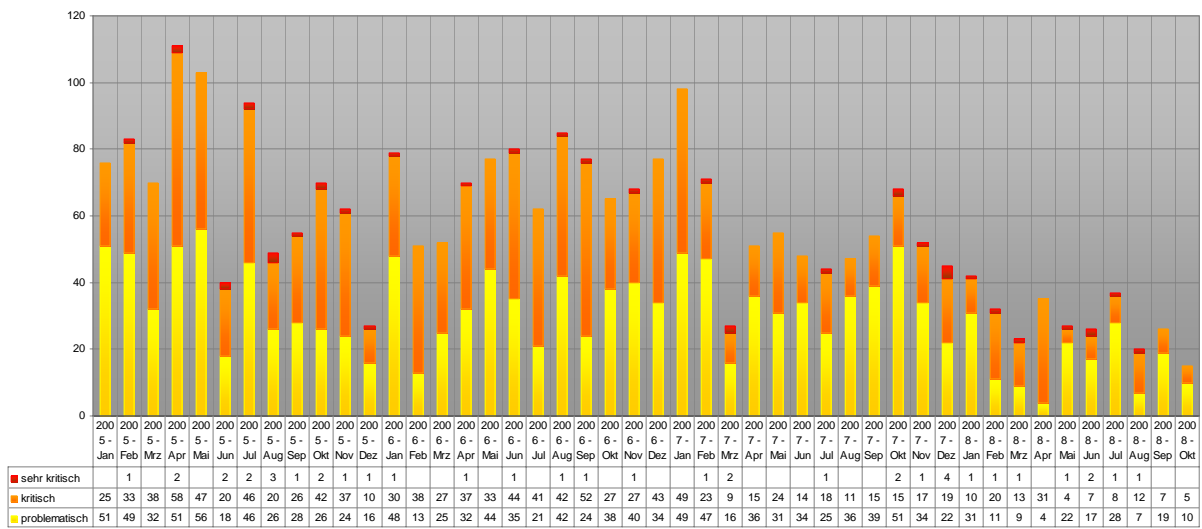
Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2008

Registrierte Schwachstellen by scip AG



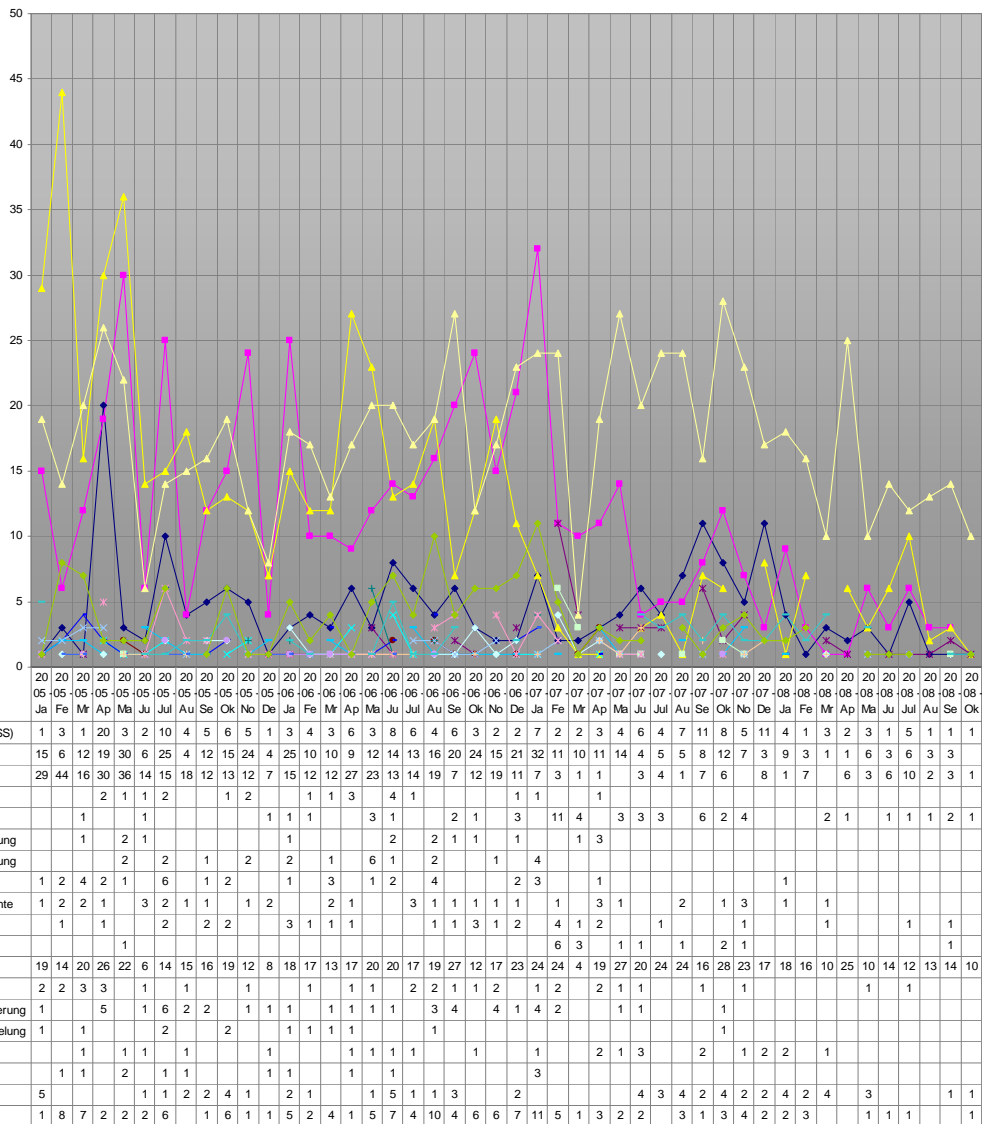
Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005

scip monthly Security Summary 19.10.2008



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005





Verlauf der Anzahl Schwachstellen/Kategorie pro Monat seit Januar 2005

5. Bilderrätsel



GESUCHTE BEGRIFFE		
5 (engl.)	11 Buchstaben (engl.)	7 Buchstaben (engl.)

LÖSUNGSWORT

Wettbewerb

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

Einsendeschluss ist der **15.11.2008**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung des Bilderrätsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary > Errata.

Gewinnen Sie einen Monat des [Securitytracker](#) Dienstes **)pallas(**.

SECURITYTRACKER



6. Impressum

Herausgeber:



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

Zuständige Person:



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

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich IT-Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserungen möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch. Das **Errata** (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summaries finden Sie online. Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)