

Contents

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

1. Editorial

Backdooring wird stets unterschätzt

Jetzt mal ehrlich: Jeder von uns verwendet irgendwie und irgendwo closed-source Software. Also eine Anwendung, deren Quellen und interne Funktionsweise nicht einsehbar sind. Dies bedeutet, dass wir als Endanwender vor einer mysteriösen "Blackbox" sitzen, die wir nicht verstehen können, an die wir blind glauben müssen. Wahrscheinlich sitzen Tag für Tag mehr "Gläubige" vor einem Computer, weder in der Kirche.

"Wieso hackt der nun wieder auf closed-source rum? Es ist doch alles nur halb so schlimm?" wird sich der eine oder andere Fragen. Nein, ich bin kein religiöser Fundamentalist, der seinen open-source Fanatismus zur Schau stellen muss. Viel mehr geht es darum aufzuzeigen, dass geschlossene Produkte immer ein unkalkulierbares Risiko in sich bergen.

Gehen wir davon aus, wir sind ein Unternehmen, dem Sicherheit am Herzen liegt. Wir kaufen von

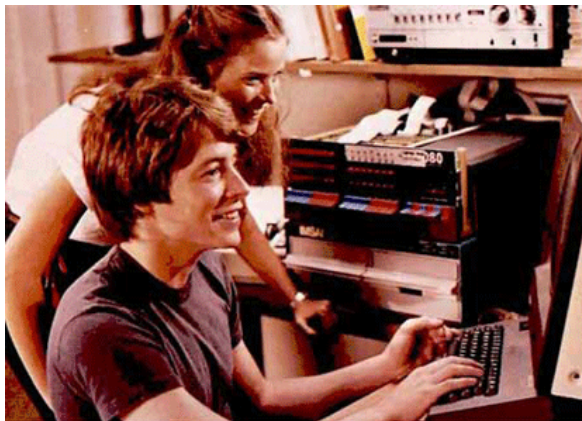
einer israelischen Firma (die Herkunft derer ist rein zufällig gewählt) ein Sicherheitsprodukt ein. Es handelt sich dabei um ein ausgeklügeltes Authentisierungs-System, das durch Best Practice-Ansätze und State of the Art-Mechanismen ein Höchstmass an Sicherheit gewährleisten will. Ein kleines Beispiel einer solchen Anwendung habe ich hier (Binary und Sourcen) bereitgestellt.

Nun ist es so, dass sich hier nur jemand mit einem legitimen Login authentisieren kann. Ohne das Wissen um den Benutzernamen und das geheime Passwort wird man sich nicht anmelden können. Der von uns eingerichtete Benutzer lautet "admin" und dessen Passwort lautet "secret". Da wir diese Information für uns behalten, wird sich da niemand einfachso anmelden können. Wir jubeln, denn wir haben ein tolles Produkt. Die israelische Firma jubelt auch, denn die hat dafür unser gutes Geld gekriegt.

Die Firma in Israel ist aber nicht ganz so lieb und dachte sich: "Okay, vielleicht wollen wir uns trotzdem irgendwann mal anmelden. Wer weiss, vielleicht macht unser Kunde irgendwann Geschäfte mit dem bösen Iran?". Aus diesem Grund hat einer der Entwickler eine Hintertür eingerichtet. Schreibt er in das erste Feld den Benutzernamen "backdoor" und klickt auf die Taste F12, wird er auch ohne legitimes Konto authentisiert...!

Das Problem ist, dass man eine solche Hintertür nur mit erheblichem Aufwand entdecken kann.

In einem Real-World Test müsste man alle möglichen Eingaben und Abläufe durchprobieren. Die Hintertür könnte aber auch durch das dreimalige Klicken auf den Login-Button, die Eingabe von "stfu23" in das Passwortfeld und das Drücken der Tastenkombination Ctrl+Alt+4+2 aktiviert werden. Ein Ding der Unmöglichkeit, dies zeitnah herauszufinden!



Alternativ könnte man versuchen durch ein Disassemblieren der Binaries ein Reversing durchzusetzen. Mit viel Aufwand und Wissen könnte man die Hintertür ausmachen. Doch bis dann existieren wahrscheinlich entweder Israel oder der Iran in der gegenwärtigen Form nicht mehr. Oder unser fiktives Unternehmen wurde durch einen amerikanischen Konzern übernommen und wir mittlerweile durch indische Entwickler ersetzt.

Wäre die Anwendung quelloffen und damit eine Source Code Analyse möglich, könnte man mit relativ wenig Aufwand die unliebsamen Codeteile ausfindig machen. Ein geübter Analyst sähe eine Prozedur wie folgende spätestens auf den zweiten Blick:

```
Private Sub txtUser_KeyUp(KeyCode As Integer, Shift As Integer)
If (txtUser.Text = "backdoor" And KeyCode = 123) Then
MsgBox "You are authenticated with the secret backdoor sequence!", vbCritical, "Authentication successfull"
End If
End Sub
```

Längerfristig ist es nur ein Vorteil, wenn eine Anwendung offen angeboten wird. Im Bereich und zu Gunsten der Sicherheit ist es gar eine Pflicht! Doch nach wie vor haben das viele Firmen und Organisationen nicht verstanden. Da werden geschlossene VPN-Lösungen aus Übersee eingekauft, die dubiose HTTP-Ports an der externen Schnittstelle anbieten, die ihrerseits angeblich keinen Nutzen haben (wieso sind sie denn vorhanden?!). Oder halt die Schweizer Armee, die irgendwelche Technologiespielereien aus dem Heiligen Land einkauft und sich dabei auf die Zusicherung verlässt, dass alles mit rechten Dingen zugeht. Kein Wunder werden die westlichen Nachrichtendienste seit Jahrzehnten durch den Mossad belächelt (siehe hierzu die nicht unumstrittenen Enhüllungen von Viktor Ostrovsky).

Bekanntlich sind aber in der Liebe und im Krieg alles erlaubt... Und nur weil man nicht mitbekommt, dass andere Menschen böse Dinge planen und durchführen, heisst es nicht, dass es sie nicht gibt. In diesem Fall ist man ja schliesslich gerade darum bemüht, dass solche Bestrebungen nie ans Tageslicht kommen. Und dank closed-source haben die Nutzer eher schlechte Karten.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 15. Dezember 2008

2. scip AG Informationen

2.1 Erfolgreiches neues Jahr

Das neue Jahr 2009 hat definitiv begonnen.

Die kurze Zeit der verbreiteten Arbeitspause ist vorüber. Täglich stehen wieder Meetings, Workshops und Entscheidungen an.

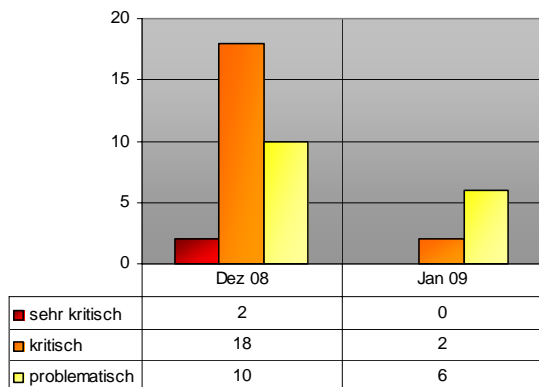
Die scip AG wünscht Ihnen auf diesem Weg noch einmal ein erfolgreiches und gesundes Jahr.

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:

- 3908 Oracle Database Critical Patch Update Jan 2009
- 3907 Cisco IOS HTTP unbekannter Parameter Cross-Site-Scripting
- 3904 OpenSSL DSA / ECDSA "EVP_VerifyFinal()" Spoofing
- 3903 SAP GUI TabOne ActiveX Control Caption List Pufferüberlauf
- 3902 VMware "vmware-authd" Denial of Service

3.1 Oracle Database Critical Patch Update Jan 2009

Einstufung: **kritisch**
 Remote: Ja
 Datum: 15.01.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3908>

Oracle Database (auch Oracle Database Server, Oracle RDBMS o. ä.) ist eine Datenbankmanagementsystem-Software. Ein Oracle Datenbanksystem kann sowohl relationale Daten, als auch objektrelationale Daten speichern. Weiterhin besitzt es die Fähigkeit zur Verarbeitung und relationalen Transformation von XML-Datenstrukturen (XMLDB, XDK). Es implementiert die ACID-Eigenschaften, bietet gute Skalierbarkeit und einen sehr großen Funktionsumfang.

Oracle veröffentlichte im Januar ein Critical Patch Update, das unter anderem 10 kritische Lücken in Oracle Database schliesst. Die zugrundeliegenden Lücken sind lückenweise bekannt und wurden in der Vergangenheit besprochen.

- CVE-2008-5437
- CVE-2008-5436
- CVE-2008-3978
- CVE-2008-3979
- CVE-2008-4015
- CVE-2008-3974
- CVE-2008-3997
- CVE-2008-3999
- CVE-2008-5439
- CVE-2008-3973

Expertenmeinung:

Wie so oft sind hier leider nur wenige Details zu den effektiv gepatchten Schwachstellen erhältlich. Bei den meisten Schwächen handelt es sich aber um Probleme, die vom Hersteller wie auch den jeweiligen Researchern in der Regel als kritisch angesehen werden. Dementsprechend sei hier die Empfehlung festgehalten, das entsprechende Patchpaket so schnell wie möglich einzuspielen.

3.2 Cisco IOS HTTP unbekannter Parameter Cross-Site-Scripting

Einstufung: **problematisch**
 Remote: Ja
 Datum: 15.01.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3907>

nternetnetwork 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 Boscack, 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 Mai 2005 in der Version 12.4 vor. Ein kürzlich veröffentlichtes Advisory beschreibt eine Schwachstelle, bei der ein unbekannter Parameter nicht korrekt validiert wird, bevor er an den Benutzer zurückgeliefert wird. Dadurch lässt sich beliebiger Scriptcode im Kontext der Applikation zur Ausführung bringen.



Expertenmeinung:

Als ob man bei Cisco derzeit nicht schon genügend an Felix Lindners Vortrag zur zuverlässigen Ausnutzung von IOS Bugs zu kämpfen hätte, kommen diese relativ grundlegenden, aber nicht minder problematischen XSS-Schwächen sicher nicht zum idealen Zeitpunkt für den Netzwerkriesen. Basierend auf dessen Aussagen, sollten betroffene Administratoren zeitnah auf eine aktualisierte Version wechseln, um die Exponierung dieser Schwachstelle zu reduzieren.

3.3 OpenSSL DSA / ECDSA "EVP_VerifyFinal()" Spoofing

Einstufung: **kritisch**
 Remote: Ja
 Datum: 08.01.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3904>

OpenSSL ist eine freie Implementierung des SSL/TLS-Protokolls und bietet darüber hinaus weitergehende Funktionen zur Zertifikatsverwaltung und zu unterschiedlichen kryptographischen Funktionen. Es basiert auf dem SSLeay-Paket, das von Eric A. Young und Tim Hudson entwickelt wurde, und wird zurzeit von einer unabhängigen Gruppe weiterentwickelt. Das Google Security rapportierte unlängst eine Schwachstelle bei der der Rückgabewert der Funktion EVP_VerifyFinal() nur unzureichend geprüft wird. Dadurch kann der Signaturcheck durch eine manipulierte Signatur umgangen werden.

Expertenmeinung:

OpenSSL ist eine oft integrierte und entsprechend wichtige Komponente vieler Softwareprodukte, was diese Schwachstelle mehr als problematisch erscheinen lässt. Betroffene Applikationen sollten umgehend gepatcht werden. Desweiteren sollte überprüft werden, ob eventuelle Bundle-Versionen der Applikation vorhanden sind, die diese Schwäche enthalten.

3.4 SAP GUI TabOne ActiveX Control Caption List Pufferüberlauf

Einstufung: **problematisch**
 Remote: Ja
 Datum: 08.01.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3903>

Die SAP AG ist der größte europäische und

weltweit viertgrößte Softwarehersteller. Der Hauptsitz befindet sich im badischen Walldorf (Rhein-Neckar-Kreis). Tätigkeitsschwerpunkt ist die Entwicklung von Software für Unternehmen zur Abwicklung der gesamten Geschäftsprozesse eines Unternehmens, darunter Buchhaltung, Logistik und Personalwesen. Carsten Eiram von Secunia fand eine Schwachstelle in SAPGui, bei der durch einen Pufferüberlauf beliebiger Code zur Ausführung gebracht werden kann. Dadurch wird eine Kompromittierung des Systems ermöglicht.

Expertenmeinung:

SAP Gui ist grundsätzlich ein, vor allem im Finanzumfeld verbreitetes, Werkzeug zur Verwendung mit verschiedenen SAP-Lösungen. Dementsprechend sollte die vorliegende Schwachstelle zeitnah adressiert werden, um eine Ausnutzung zu vermeiden.

3.5 VMware "vmware-authd" Denial of Service

Einstufung: **problematisch**
 Remote: Ja
 Datum: 07.01.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3902>

VMware, Inc., ist ein US-amerikanisches Unternehmen, das Software im Bereich der Virtualisierung herstellt. Die Firma 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. Durch einen Fehler im vmware-authd kann ein Angreifer einen Denial of Service auslösen. Der Fehler liegt dabei in der Bearbeitung von überlangen Zeichenketten.

Expertenmeinung:

Ein relativ primitiver Fehler führt hier zu einem Denial of Service Fehler, der durch die Verfügbarkeit eines Exploits auch relativ einfach auszunutzen ist. Entsprechend rasch sollte die Adressierung des Problems durch den entsprechenden Patch angegangen werden, um das Risiko einer Ausnutzung zu reduzieren.

4. Statistiken Verletzbarkeiten

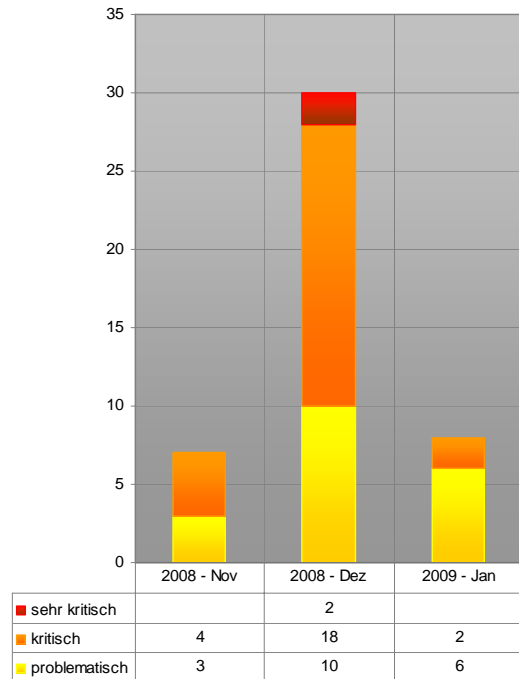
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



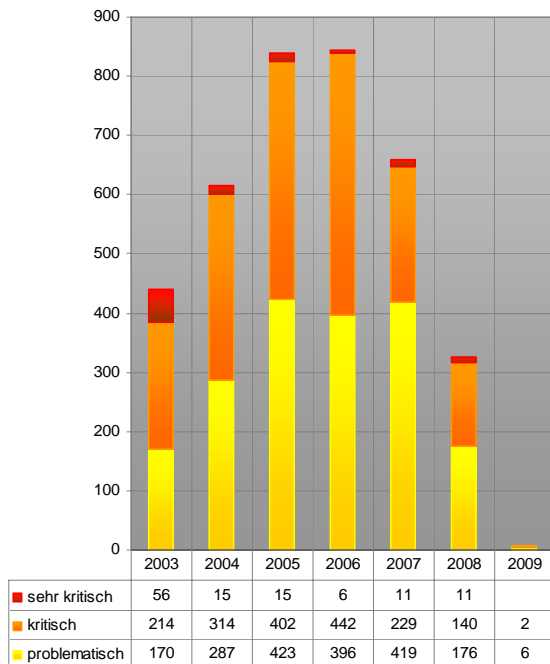
<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

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.

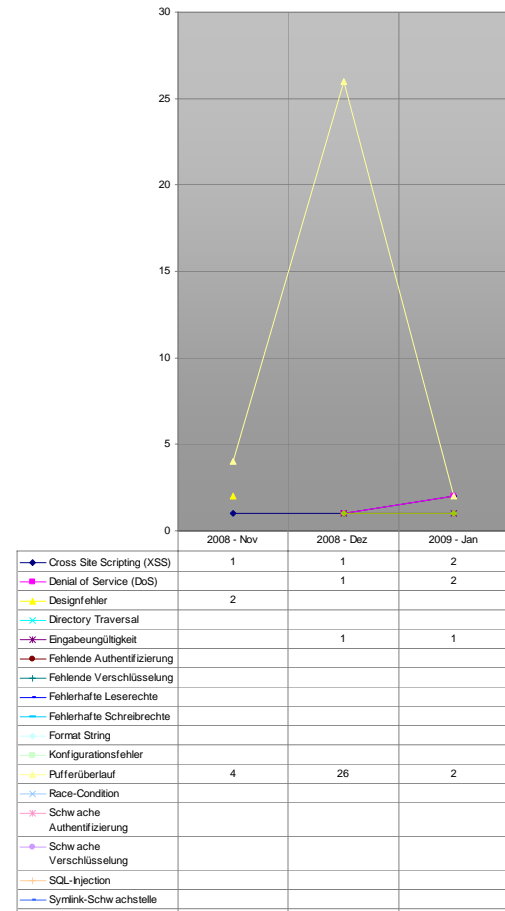
Auswertungsdatum: 19. Januar 2009



Verlauf der Anzahl Schwachstellen pro Jahr

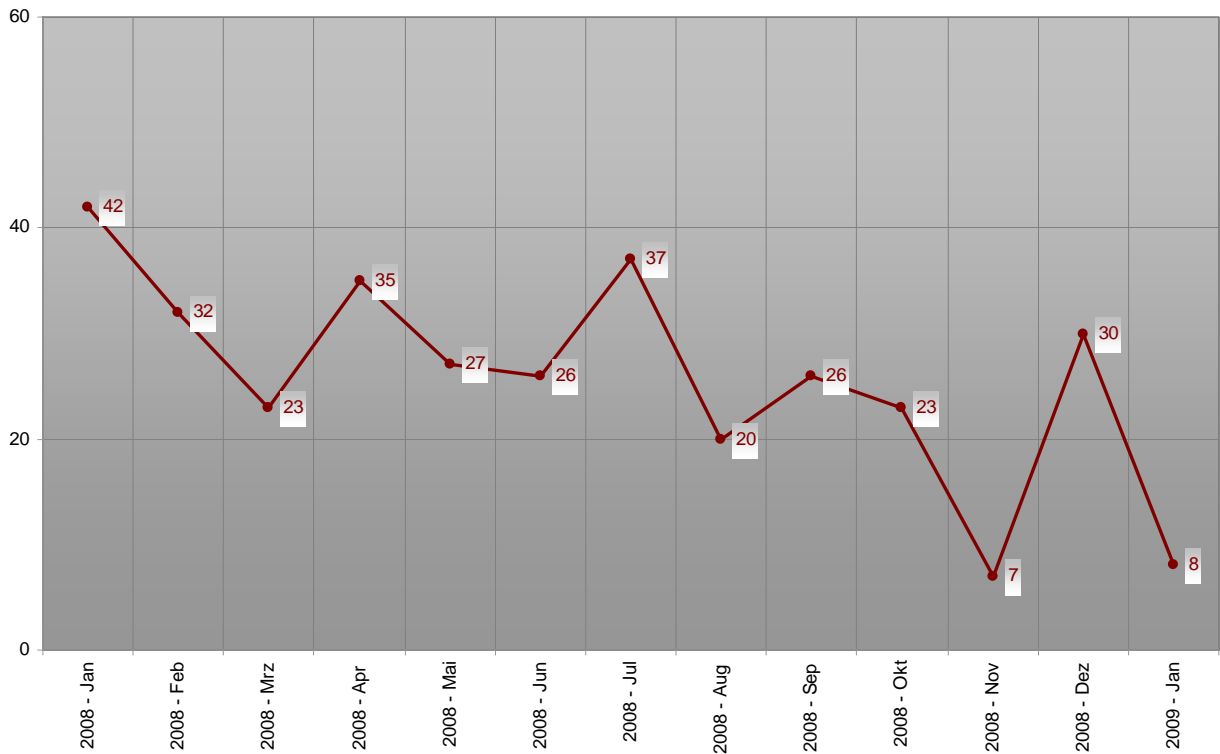


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

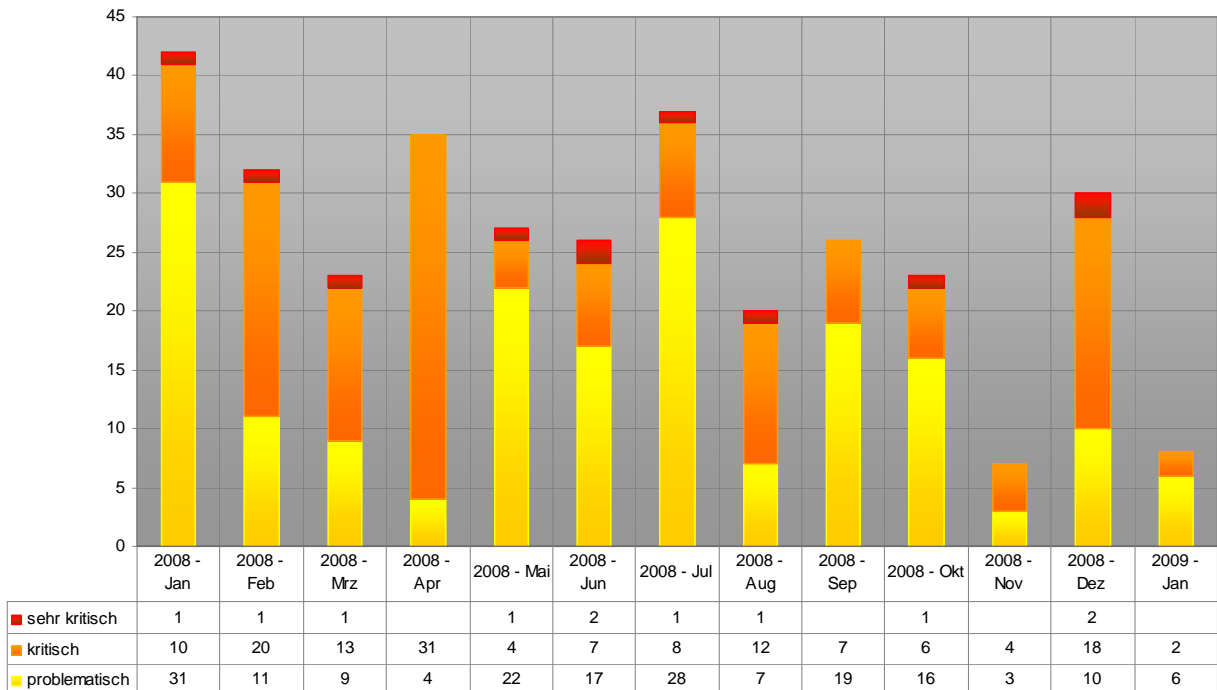


Verlauf der letzten drei Monate Schwachstelle/Kategorie

Registrierte Schwachstellen by scip AG

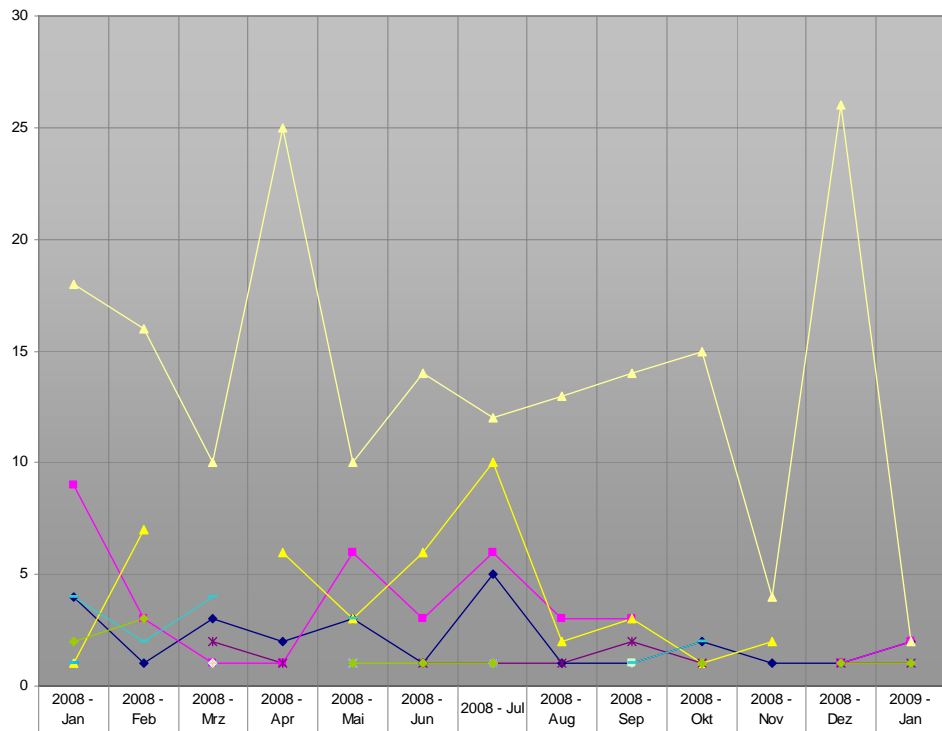


Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008-2009



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2008-2009

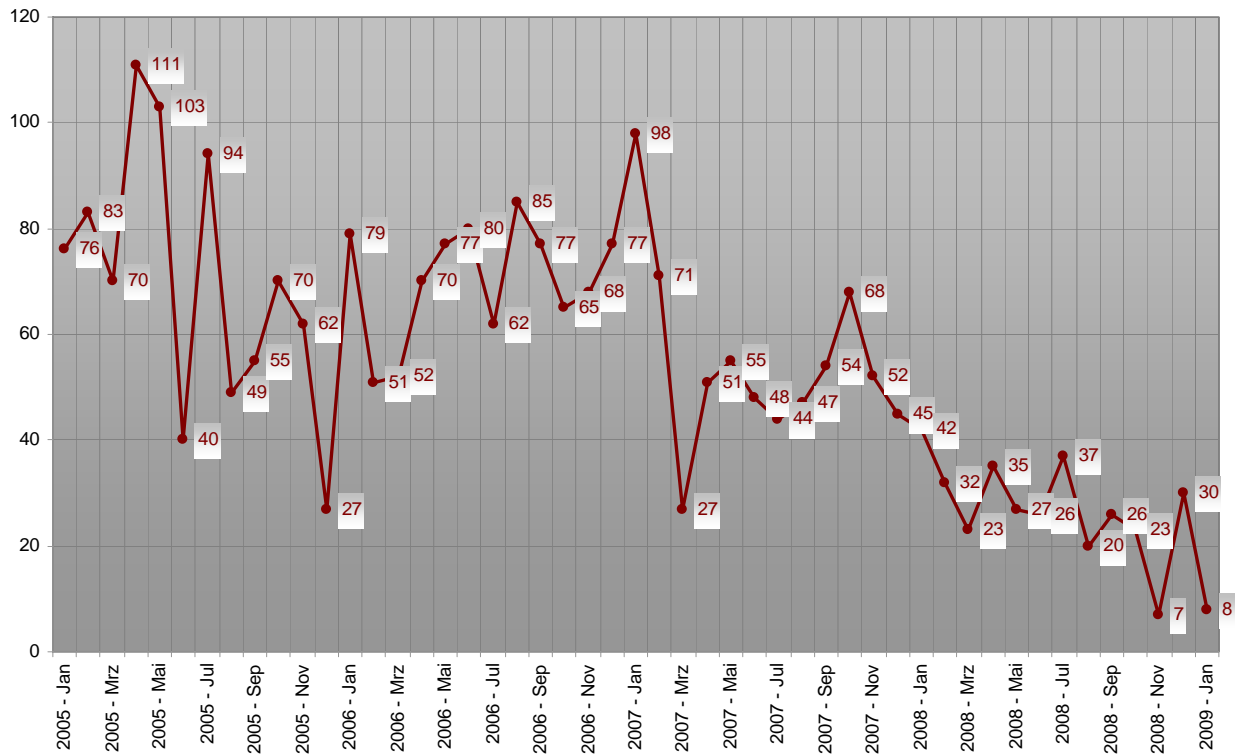




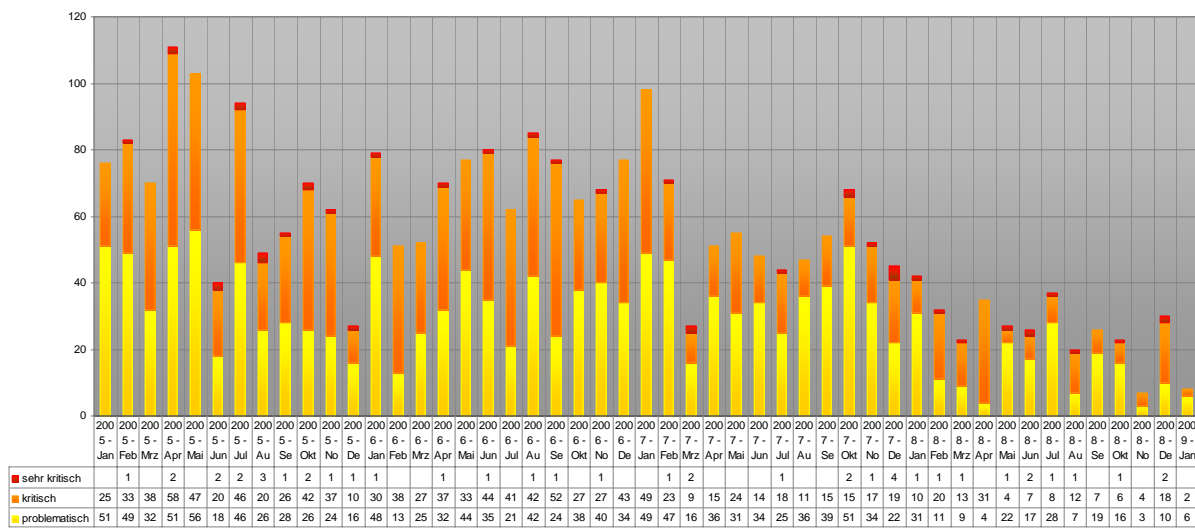
	2008 - Jan	2008 - Feb	2008 - Mrz	2008 - Apr	2008 - Mai	2008 - Jun	2008 - Jul	2008 - Aug	2008 - Sep	2008 - Okt	2008 - Nov	2008 - Dez	2009 - Jan
◆ Cross Site Scripting (XSS)	4	1	3	2	3	1	5	1	1	2	1	1	2
■ Denial of Service (DoS)	9	3	1	1	6	3	6	3	3	1	1	1	2
▲ Designfehler	1	7		6	3	6	10	2	3	1	2		
✕ Directory Traversal													
✖ Eingabeungültigkeit			2	1		1	1	1	2	1		1	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	15	4	26	2
✕ Race-Condition					1		1						
✖ Schwache Authentifizierung													
● Schwache Verschlüsselung													
— SQL-Injection	2		1							1			
— Symlink-Schwachstelle													
— Umgehungs-Angriff	4	2	4		3				1	2			

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2008-2009

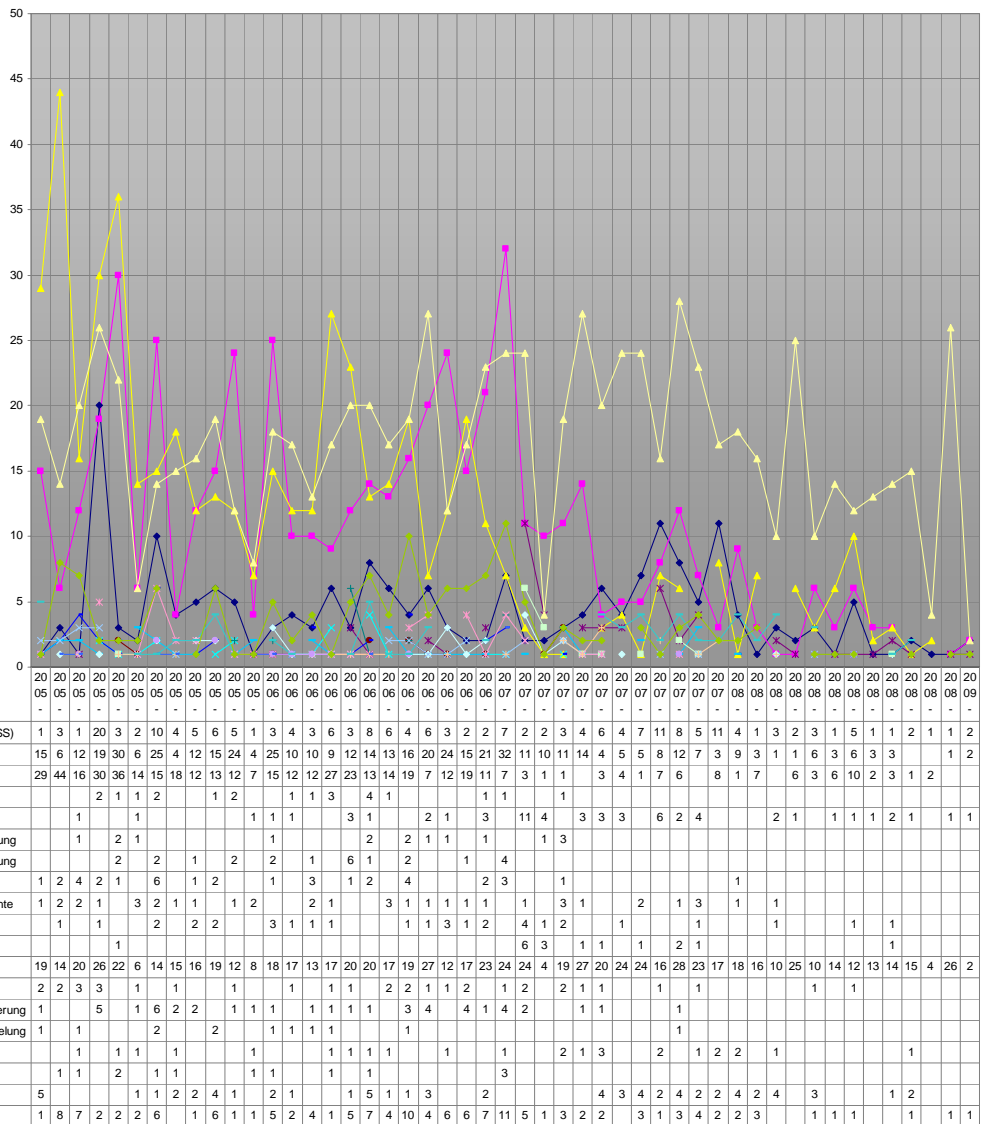
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005



Verlauf der Anzahl Schwachstellen/Kategorie pro Monat seit Januar 2005



5. Bilderrätsel



GESUCHTE BEGRIFFE		
8 (engl.)	6 Buchstaben (engl.)	9 Buchstaben (engl.)

LÖSUNGSWORT

scip monthly Security Summary 19.01.2009

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 **15.02.2009**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung des Bilderrätsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary > Errata.

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

SECURITYTRACKER



6. Impressum

Herausgeber:



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

Zuständige Person:



Marc 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!](#)