

Contents

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

1. Editorial

Intransparente Scanner und False Positives

Kurz nachdem ich im Data Becker-Verlag als Co-Autor das Buch Hacking Intern veröffentlicht hatte, habe ich mit der Übersetzung des Buchs Network Intrusion Detection von Stephen Northcutt und Judy Novak aus dem Englischen begonnen. Ich mochte das Buch, welches ich selbst vor meiner Übersetzungsarbeit mindestens drei Mal durchgelesen habe (zwei Mal auf Deutsch und einmal auf Englisch), wirklich sehr.

Dabei kann ich mich noch sehr gut daran erinnern, wie die Autoren ausdrücklich darauf hinwiesen, dass gerade im Bereich der elektronischen Erkennung die Transparenz eine ungemein wichtige Rolle spielt. Ein entsprechendes Intrusion Detection-System kann nur dann effektiv und effizient betrieben werden, wenn dessen Funktionsweise offengelegt ist: Indem die jeweiligen Rules/Pattern verstanden oder gar angepasst werden, kann eine umfassende Lösung erreicht werden. Blackbox-Systeme, bei denen man keines der beiden Dinge machen kann, widersprechen dem eigentlichen Ziel der Sicherheitsüberwachung.

Dieses Paradigma aus der elektronischen

Einbruchserkennung kann und muss genauso auf den Bereich der Sicherheitsüberprüfungen übernommen werden. Auch hier ist man, will man gewisse Dinge möglichst effektiv analysieren, auf unterschiedliche Software-Produkte angewiesen. Durch Scanner wie nmap oder Nessus können eine Vielzahl an Informationen automatisiert zusammengetragen und ausgewertet werden.

Bei unseren webbasierten Tests ziehen wir ebenfalls N-Stealth zurate. Hierbei handelt es sich um einen Web-Scanner, der ursprünglich durch den Brasilianer Felipe Moniz geschrieben wurde. Die neueste Version der Software kommt mit einigen herausragenden Funktionalitäten daher. So wird ein umfassendes Crawling des Webservers vorgenommen und auf der Basis dieses Mappings die einzelnen Test-Module dem Zielsystem angepasst (z.B. dynamische Allokation von zu prüfenden Objekten). Ich bin sehr zufrieden mit dem Produkt, welches natürlich noch punktuell verbessert werden kann. Schlussendlich bietet es aber etwas, was man sich schon vor 10 Jahren sehnlichst herbeigewünscht hat.

In einem meiner Penetration Tests wies ich sodann üblicherweise die unliebsam unterstützten HTTP-Methoden des Webservers aus. Darunter gehören klassische Methoden wie HEAD, POST, PUT, DELETE, OPTIONS, TRACE und TRACK. Aber auch Erweiterungen aus WebDAV, zum Beispiel PROPFIND und MOVE, konnte ich nebenbei im Rahmen des N-Stealth Scans als unterstützt ausmachen. Dies, und andere, weitaus kritischere Probleme, teilte ich dem Kunden mit. Mit der Abgabe unseres Reports war er sogleich darum bemüht, die eben genannten Probleme zu beheben.

Nach der Umsetzung bat er mich, wenigstens kurz zu prüfen, ob nun die HTTP-Methoden korrekt gesetzt sind. Da ein solcher Re-Check eigentlich jeweils Teil eines neuen Projekts ist und nicht in der initialen Prüfung enthalten, habe ich nur kurz im Hintergrund N-Stealth angeworfen und auf die Resultate gewartet. Noch immer wurden mir PROPFIND & co. als "supported" ausgewiesen. In einem kurzen Mail wies ich den Kunden darauf hin, dass er das Problem wohl noch nicht richtig adressiert hätte.



In seiner Antwort bat er um konkrete Hilfestellung, wie die Konfigurationseinstellungen unter Apache auszusehen hätten. HTTP-Methoden können dabei sowohl innerhalb einer .htaccess-Datei als auch in der httpd.conf deaktiviert werden. Ebenso wies er mich darauf hin, dass in seinen manuellen Tests mittels Telnet die beanstandeten Methoden nur noch ein 403 Forbidden liefern würden. Also machte ich mich daran, nachdem ich die Konfigurationsmöglichkeiten dokumentiert hatte, die Unterstützung der HTTP-Methoden manuell zu verifizieren.

Zu meinem Erstaunen lieferten, abgesehen von einer speziellen Form von OPTIONS, alle kritischen Methoden nur noch ein 403 Forbidden zurück. Das System war also eigentlich gehärtet. Aber wieso meldete mir N-Stealth noch immer, dass sie unterstützt seien? Um der Sache auf den Grund zu gehen, habe ich einen erneuten Scan initiiert und diesen mittels Wireshark mitgeschnitten. Ich wollte sehen, ob die Anfragen der Scanning-Software irgendwie anders waren, weder meine manuellen Zugriffe.

Zu meinem Erstaunen wurden die exakt gleichen Anfragen verwendet, die zu den exakt gleichen Resultaten - nämlich dem gewünschten Forbidden - führen sollten. Es schien, als hätte N-Stalker irgendein Problem bei der Auswertung von HTTPS-Webservern. Da die Test-Prozeduren weder im Detail einsehbar noch im Report umfassend dokumentiert waren, musste ich also zuerst langwierig eine Netzwerkanalyse einspannen, um dem Mysterium auf den Grund zu gehen. Ich schrieb sofort ein Email an die Entwickler und informierte meinen Kunden über die unschöne Ungenauigkeit.

Uneingeschrenkte Transparenz bleibt sehr wichtig, um Software und ihre Funktionsweise verstehen zu können. Letzteres ist unabdingbar, um im Sicherheitsbereich intelligent agieren zu können. Und irgendwie führt mich diese ganze Geschichte zu einem meiner alten Grundsätze, den ich ursprünglich eher selbstironisch postuliert hatte, zurück:

"Traue nie einer Software, die Du nicht selber in schlechtem Stil programmiert hast."

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 10. November 2008

2. scip AG Informationen

2.1 Source Code Review

Software bestimmt unseren Alltag. Sei dies nun in der Auslösung von Finanztransaktionen, dem Verfassen einer E-Mail, der täglichen Arbeitszeiterfassung oder der Konfiguration eines Web-servers. Eine Applikation versteht sich selbst als eine Aneinanderreihung von Funktionen zur Bewältigung eines wohlgeformten Problems. Dabei kommt eine zusätzliche Logik, die sich für Entscheidungen innerhalb der Verarbeitung verantwort-lich zeichnet, zum Einsatz.

Vorzugsweise in sicherheitskritischen Bereichen stellen sich nun etliche Fragen wie z.B. ob ein Angreifer aus dem ihm durch die Software zuge-wiesenen Kontexte ausbrechen kann und da-durch seine Privilegien erweitern kann oder ob er gar durch das Ausnutzen programmiertechni-scher Fehler Zugriff auf das System an sich er-langen kann.

Diese und andere Fragestellungen können durch Source Code Reviews beantwortet werden. Ent-sprechend den Vorgaben des Kunden und der zu prüfenden Software werden unterschiedliche Test umgesetzt. Eine kleine Auswahl ist nachfol-gend aufgelistet:

- Algorithmisches Debugging
- Delta Debugging
- Explizites Debugging
- Statisches Debugging
- Statistisches Debugging
- Program Slicing

Dank unserer langjährigen Erfahrung in diesem Fachgebiet inklusive der Programmierung eigen-er Analysesoftware und unserem ausgewiese-nen Expertenwissen haben wir als scip AG die Ehre die unterschiedlichsten Applikationen (Re-verseProxy, Transaktionsapplikation etc.) nam-hafter nationaler- und internationaler Unterneh-mungen 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

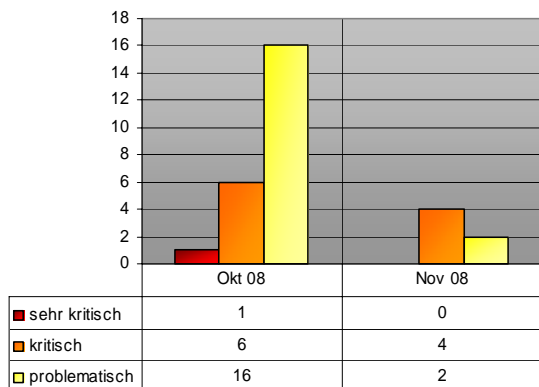
Gerne können wir Ihre Anliegen besprechen.

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:

- 3867 VMware Produktserie Trap-Flag Privilege Escalation
- 3866 Microsoft Windows SMB Authentication Credential Replay
- 3865 VLC Media Player RealText Demuxer Pufferüberlauf
- 3864 VLC Media Player CUE Demuxer Pufferüberlauf
- 3863 Adobe Acrobat/Reader "util.printf()" Pufferüberlauf
- 3862 phpMyAdmin "db" Cross-Site Scripting
- 3861 Cisco ASA and PIX VPN Umgehung der Authentisierung
- 3860 Microsoft Windows Path Canonicalisation Schwachstelle
- 3859 Trend Micro OfficeScan CGI Parsing Pufferüberlauf
- 3858 VLC Media Player TY Processing Pufferüberlauf
- 3856 RealVNC VNC Viewer "CMsgReader::readRect()" Encoding Type Schwachstelle

3.1 VMware Produktserie Trap-Flag Privilege Escalation

Einstufung: **problematisch**
 Remote: Ja
 Datum: 17.11.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3867>

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. Derek Soeder entdeckte eine Schwachstelle, bei der durch einen Fehler in der CPU Hardware Emulation ein Trapflag nicht richtig verarbeitet wird und dadurch das Erlangen erweiterter Rechte durch einen Angreifer begünstigt.

Expertenmeinung:

Auch wenn diese Schwachstelle bedingt, dass ein Benutzer lokalen Zugriff zu einem Gast-Betriebssystem besitzt, ist sie sicherlich nicht als gänzlich unkritisch anzusehen und sollte zeitnah behandelt werden. Es empfiehlt sich, das Patch-Paket von VMWare zeitnah einzuspielen.

3.2 Microsoft Windows SMB Authentication Credential Replay

Einstufung: **kritisch**
 Remote: Ja
 Datum: 11.11.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3866>

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. Microsoft meldete unlängst eine Schwachstelle, bei der durch das Aufzeichnen und Wiedergeben von SMB Authentisierungsinformationen erweiterter Zugang zu geschützten Bereich des Systems erreicht werden konnte.

Expertenmeinung:

Und wieder eine kritische Schwachstelle, die diversen Administratoren die eine oder andere Überstunde verschaffen dürfte. Im Gegensatz zu vorhergehenden, kritischen, Lücken ist diese Schwachstelle nur unter gewissen Konditionen auszunutzen und daher nicht hochkritisch. Dennoch sollte das Einspielen des entsprechenden Patches möglichst zeitnah ein Angriff genommen werden.



3.3 VLC Media Player RealText Demuxer Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 06.11.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3865>

Der VLC media player (anfänglich VideoLAN Client) ist ein portabler, freier Media Player sowohl für diverse Audio-, Videocodecs und Dateiformate als auch DVDs, Video-CDs und unterstützt unterschiedliche Streaming-Protokolle. Er kann auch als Server zum Streaming in Uni- oder Multicast in IPv4 und IPv6 verwendet werden. Tobias Klein beschreibt in einem Advisory eine Schwachstelle, bei der ein Fehler im RealText Demuxer zu einem Pufferüberlauf führt, der die Ausführung beliebigen Codes über ein manipuliertes Videofile erlaubt.

Expertenmeinung:

VLC ist heute eine Standardapplikation, die sich sowohl im Power- wie auch im Endusersegment grosser Beliebtheit. Die vorliegende Schwachstelle ist aufgrund der hohen Verbreitung als kritisch anzusehen und sollte entsprechend zeitnah adressiert werden. Als Gegenmassnahme wäre hier lediglich das Einspielen des entsprechenden Updates zu empfehlen.

3.4 VLC Media Player CUE Demuxer Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 06.11.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3864>

Der VLC media player (anfänglich VideoLAN Client) ist ein portabler, freier Media Player sowohl für diverse Audio-, Videocodecs und Dateiformate als auch DVDs, Video-CDs und unterstützt unterschiedliche Streaming-Protokolle. Er kann auch als Server zum Streaming in Uni- oder Multicast in IPv4 und IPv6 verwendet werden. Tobias Klein beschreibt in einem Advisory eine Schwachstelle, bei der ein Fehler im CUE Demuxer zu einem Pufferüberlauf führt, der die Ausführung beliebigen Codes über ein manipuliertes Videofile erlaubt.

Expertenmeinung:

VLC ist heute eine Standardapplikation, die sich sowohl im Power- wie auch im Endusersegment grosser Beliebtheit. Die vorliegende

Schwachstelle ist aufgrund der hohen Verbreitung als kritisch anzusehen und sollte entsprechend zeitnah adressiert werden. Als Gegenmassnahme wäre hier lediglich das Einspielen des entsprechenden Updates zu empfehlen.

3.5 Adobe Acrobat/Reader "util.printf()" Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 04.11.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3863>

Adobe Reader (früher Acrobat Reader) ist ein Computerprogramm der Firma Adobe zum Anzeigen von PDF-Dokumenten, also ein Dateibetrachter. Es ist Teil der Adobe-Acrobat-Produktfamilie. Es kann kostenlos aus dem Internet heruntergeladen werden und wird von vielen Softwareherstellern zusammen mit der Dokumentation ihrer Programme auf CD-ROMs geliefert. Von der Version 5.1 bis Version 6 war das Programm in zwei Versionen erhältlich, einer kompakten Basisversion und einer erweiterten Version, die neben dem Anzeigen von Dokumenten auch Volltextsuche (mit beigefügtem Index auch von PDF-Dokumentensammlungen) und die Wiedergabe eingebetteter Multimediaobjekte unterstützt. Seit der Version 7 können auch dreidimensionale Grafikobjekte angezeigt werden. Bestimmte Funktionen stehen nur in Dokumenten zur Verfügung, die mit dem kostenpflichtigen Adobe Reader Extension Server freigeschaltet wurden. Neben der Funktionen Anzeigen und Drucken von Dokumenten unterstützt der Adobe Reader auch das Ausfüllen von Formularen. Diese können ausgedruckt werden und, wenn der Verfasser des Dokuments dies freigeschaltet hat, auch gespeichert oder als E-Mail an eine vorgegebene Adresse geschickt werden. Auch die Funktionen Anmerken und Kommentieren müssen freigeschaltet werden. Dyon Balding publizierte unlängst eine Schwachstelle in aktuellen Versionen der Software, die aufzeigte, dass ein Angreifer mittels eines manipulierten PDF Files und der darin eingebetteten Funktion util.printf() einen Pufferüberlauf auf dem Zielsystem ausnutzen und damit das Zielsystem kompromittieren kann.

Expertenmeinung:

Und wieder einmal sollte gut achtgegeben werden, wenn es darum geht unbekannte PDF Dokumente zu öffnen. Das Deaktivieren von Javascript ist immer noch empfohlen, auch wenn dadurch möglicherweise die Funktionalität



einiger Dokumente eingeschränkt wird. Desweiteren empfiehlt sich das umgehende Einspielen des verfügbaren Patches.

3.6 phpMyAdmin "db" Cross-Site Scripting

Einstufung: **problematisch**
 Remote: Ja
 Datum: 28.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3862>

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. Aufgrund eines Eingabefehlers, den Hadi Kiamarsi entdeckte, kann ein Angreifer mittels des Parameters "db" beliebige XSS-Angriffe durchführen, was Tür und Tor für alle derzeit bekannten Angriffstechniken auf den Browser des aktuellen Benutzers öffnet.

Expertenmeinung:

phpMyAdmin ist mittlerweile ein populäres Ziel für XSS Angriffe geworden, was im Anbetracht des Umfangs der Applikation auch nicht ganz unverständlich ist. Es sei empfohlen, hier baldmöglichst ein Update einzuspielen, um die Exponierung zu reduzieren.

3.7 Cisco ASA and PIX VPN Umgehung der Authentisierung

Einstufung: **problematisch**
 Remote: Ja
 Datum: 23.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3861>

Die Firma Cisco Systems, Inc. ist der größte Netzwerkausrüster weltweit. Bekannt ist das Unternehmen vor allem für seine Router und Switches, die einen großen Teil des Internet-Backbones versorgen. In aktuellen Versionen der PIX und ASA Appliance Serie kann durch einen Fehler, der nicht näher spezifiziert wurde, die Authentisierung umgangen werden um Zugriff auf sensitive Daten zu erlangen.

Expertenmeinung:

"Unschön" ist sicherlich eine treffende Bezeichnung für die vorliegende Schwachstelle, die Cisco nun kommentarlos und ohne Angabe

von Details hier schliesst. Auch hier gilt es wieder einmal, ohne Einzelheiten zu kennen, blind vertrauend die neusten Patches einzuspielen, um das Risiko einer Ausnutzung zu vermeiden.

3.8 Microsoft Windows Path Canonicalisation Schwachstelle

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 23.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=3860>

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. Unlängst meldete Microsoft eine massive Schwachstelle in der Datei netapi32.dll, bei der durch eine fehlerhafte Behandlung von Pfaden eine Pufferüberlauf auftrat, der mittels RPC ausgenutzt werden konnte. Nach einigen Wirren über den effektiven Impact und die Reliablility der Schwachstelle, wurde bekannt dass auf einigen Zielsystemen ein autorisierter Benutzer notwendig ist (z.B. Vista/Server 2008) während die Schwachstelle anderweitig auch ohne legitimen Benutzer ausgenutzt werden konnte. Bei einem erfolgreichen Exploit kann ein Angreifer beliebigen Code zur Ausführung bringen.

Expertenmeinung:

*** Diese Schwachstelle wurde am 4. November auf die Stufe "sehr kritisch" eskaliert ***

Viel Verwirrung herrschte im Umfeld dieser Schwachstelle, vor allem im Anbetracht der effektiven Ausnutzungsgefahr. Nachdem ursprünglich von einem 0-Day die Rede war, der lediglich spezifische regional abhängige Versionen betreffen sollte und zudem einen autorisierten Benutzer erfordern würde, ist mittlerweile bekannt dass die Schwachstelle relativ breit gestreut eingesetzt werden kann. Wir empfehlen daher das sofortige Einspielen entsprechender Updates sowie das Ergreifend zusätzlicher Massnahmen (z.B. Firewalling) zur Minimierung der Exposition schützenswerter Systeme.

3.9 Trend Micro OfficeScan CGI Parsing Pufferüberlauf

Einstufung: **problematisch**
 Remote: Ja
 Datum: 22.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3859>

Das japanische Unternehmen Trend Micro Incorporated, gelistet im Nikkei 225, ist ein weltweit agierender Anbieter von Software und Dienstleistungen in den Bereichen Virenschutz für Netzwerke, Anti-Spam und Internet Content Security. Trend Micro wurde 1988 in Kalifornien von dem gebürtigen Taiwaner Steve Chang gegründet und hat seinen Hauptsitz in Tokio. In 30 Ländern arbeiten über 3.200 Angestellte für das Unternehmen (2007). 2007 betrug der Umsatz 848 Millionen US-Dollar. Der damalige Chief Executive Officer Steve Chang übergab 2004 die Geschäftsführung an Eva Chen, Mitgründerin von Trend Micro. Trend Micro war der erste Hersteller (2004) eines plattformunabhängigen Online-Scanners. Das Produktportfolio umfasst u. a. die InterScan-Familie, OfficeScan, ScanMail, Network VirusWall und PC-cillin Internet Security. Im Produkt OfficeScan existiert eine Schwachstelle, bei der durch einen Fehler im CGI Parsing ein Pufferüberlauf provoziert werden kann, der die Ausführung beliebigen Codes begünstigt.

Expertenmeinung:

Und wieder eine Schwachstelle in einer Antivirus Lösung. Hier gilt: Updates zeitnah einspielen und so sicherzustellen, dass die Exponierung auf einem möglichst niedrigen Niveau gehalten wird.

3.10 VLC Media Player TY Processing Pufferüberlauf

Einstufung: **kritisch**
 Remote: Ja
 Datum: 20.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3858>

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. Tobias Klein fand einen Pufferüberlauf in aktuellen Versionen des Players, mit dessen Hilfe beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:

Das Dasein als Quasi-Standardapplikation ist nicht immer ganz leicht. Tobias Klein, der auch schon Bücher zum Thema Pufferüberläufe veröffentlichte, illustriert eine kritische Schwachstelle. Diese sollte zeitnah durch das Einspielen der entsprechenden Patches mitigiert werden.

3.11 RealVNC VNC Viewer "CMsgReader::readRect()" Encoding Type Schwachstelle

Einstufung: **problematisch**
 Remote: Ja
 Datum: 20.10.2008
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=3856>

Virtual Network Computing (kurz VNC) ist eine Software, die den Bildschirminhalt eines entfernten Rechners (Server) auf einem lokalen Rechner (Client) anzeigt und im Gegenzug Tastatur- und Mausbewegungen des lokalen Rechners an den entfernten Rechner sendet. Damit kann man auf einem entfernten Rechner arbeiten, als säße man direkt davor. VNC implementiert das Remote Framebuffer Protocol und ist damit, im Gegensatz zu anderer Fernwartungssoftware plattformunabhängig benutzbar. Der Hersteller meldet in aktuellen Versionen eine Schwachstelle in der Funktion "CMsgReader::readRect()", durch die beliebiger Code zur Ausführung gebracht werden kann.

Expertenmeinung:

RealVNC wird üblicherweise nicht in öffentlichen Netzen eingesetzt - zumindest sollte dies nicht der Fall sein. Dadurch hält sich die Kritikalität der vorliegenden Lücke in einem annehmbaren Rahmen. Jedoch sollte nicht vernachlässigt werden, dass die Schwachstelle für einen internen Angreifer sicherlich von Interesse sein dürfte. Ein entsprechender Patch steht bereit und sollte zeitnah eingespielt werden.

4. Statistiken Verletzbarkeiten

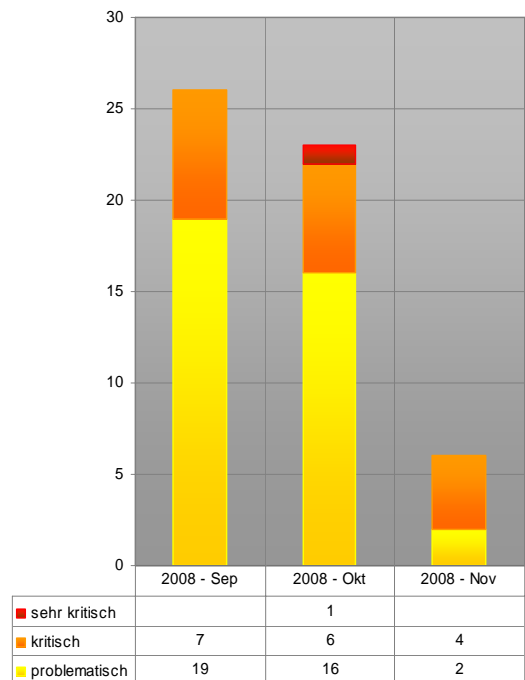
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



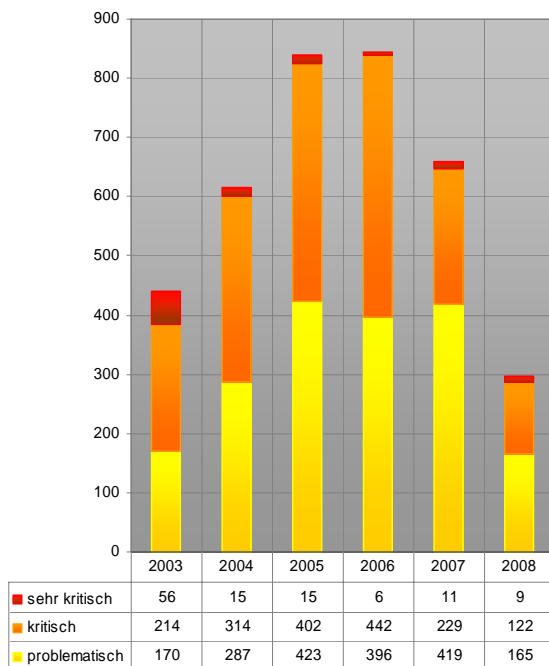
<http://www.scip.ch/cgi-bin/smss/showadvf.pl>

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.

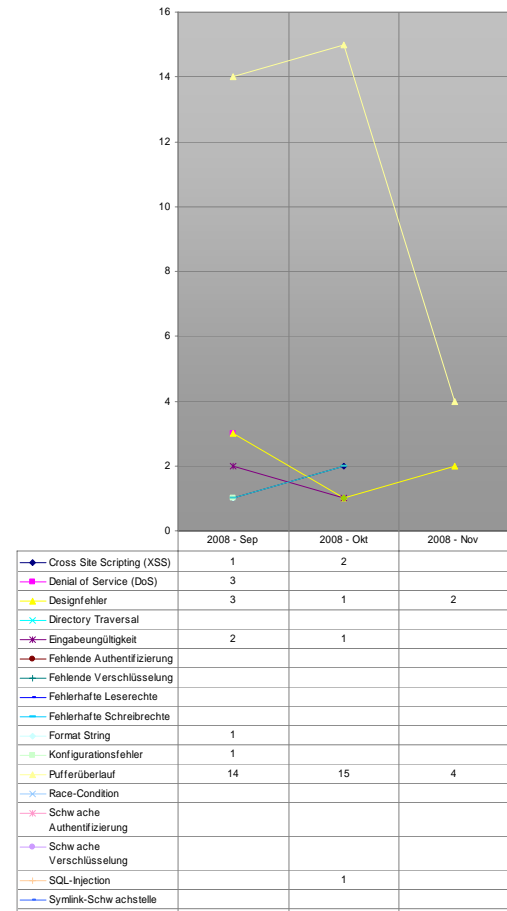
Auswertungsdatum: 19. November 2008



Verlauf der Anzahl Schwachstellen pro Jahr

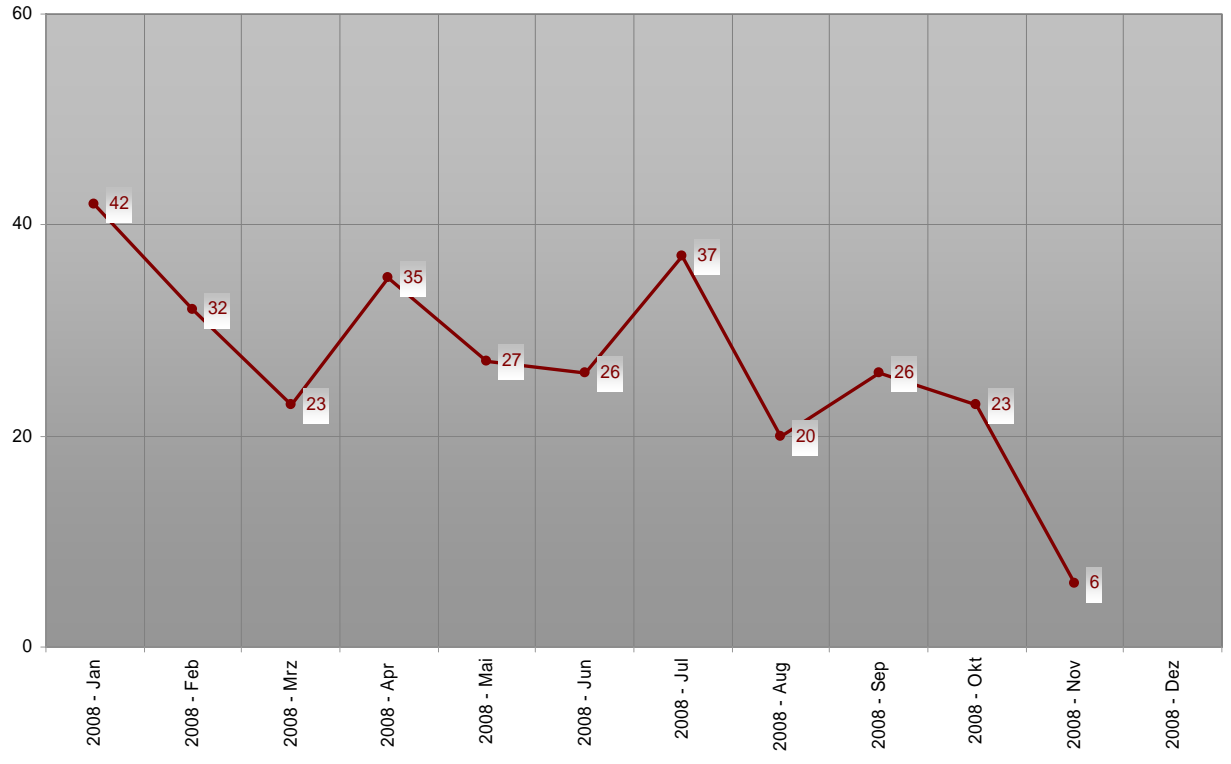


Verlauf der letzten drei Monate Schwachstelle/Schweregrad

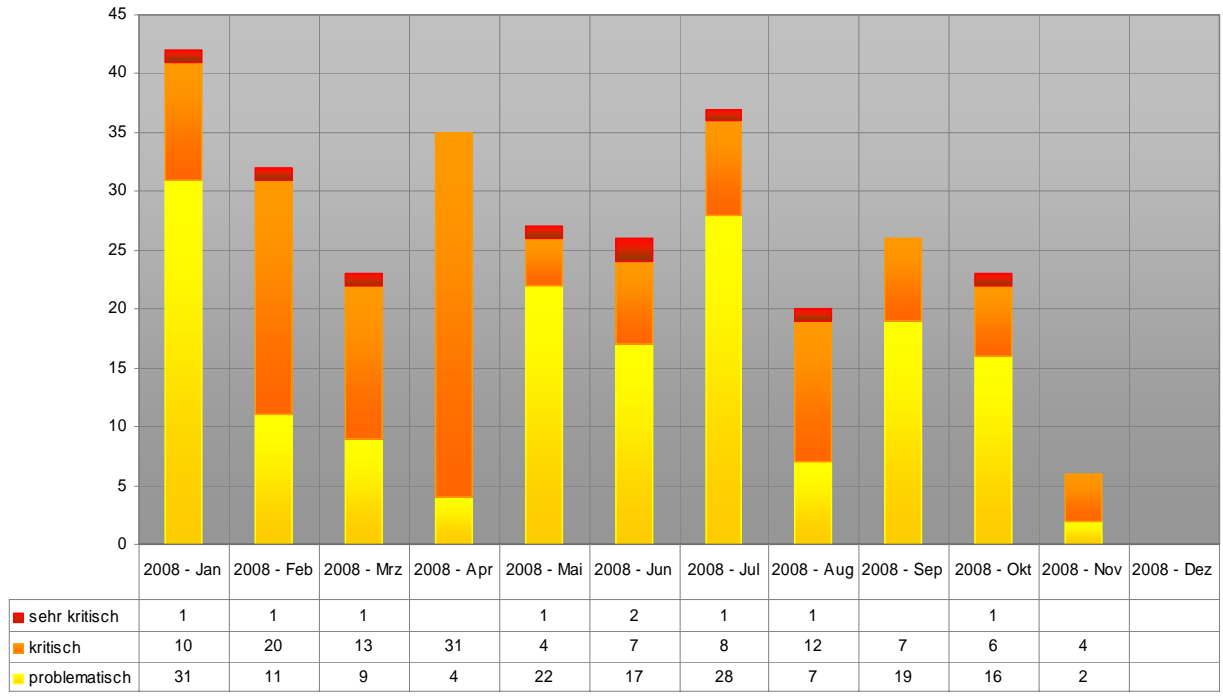


Verlauf der letzten drei Monate Schwachstelle/Kategorie

Registrierte Schwachstellen by scip AG



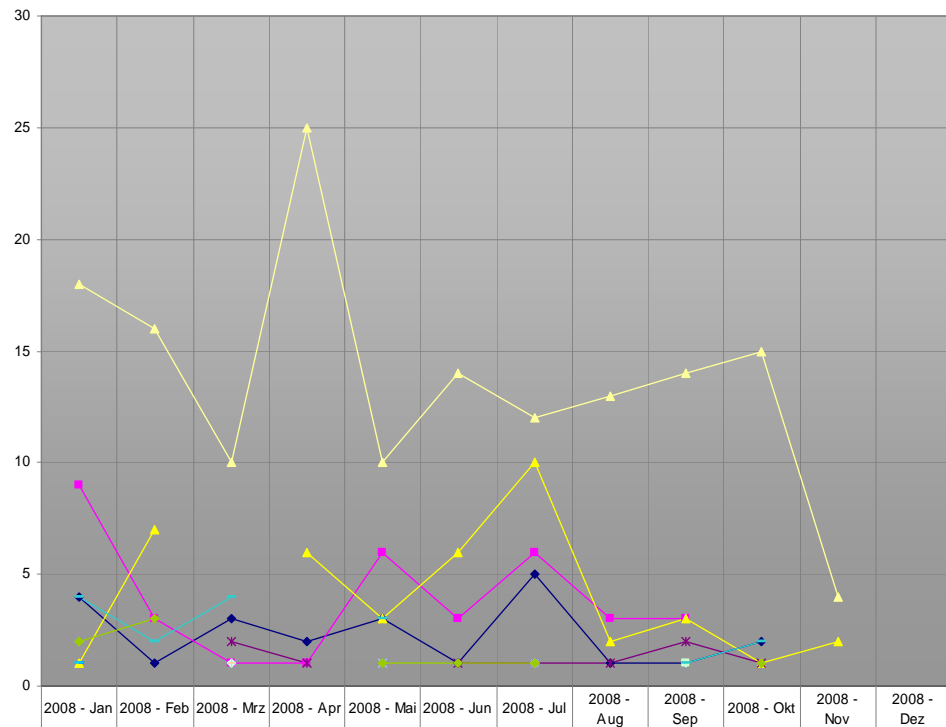
Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2008

scip monthly Security Summary 19.11.2008

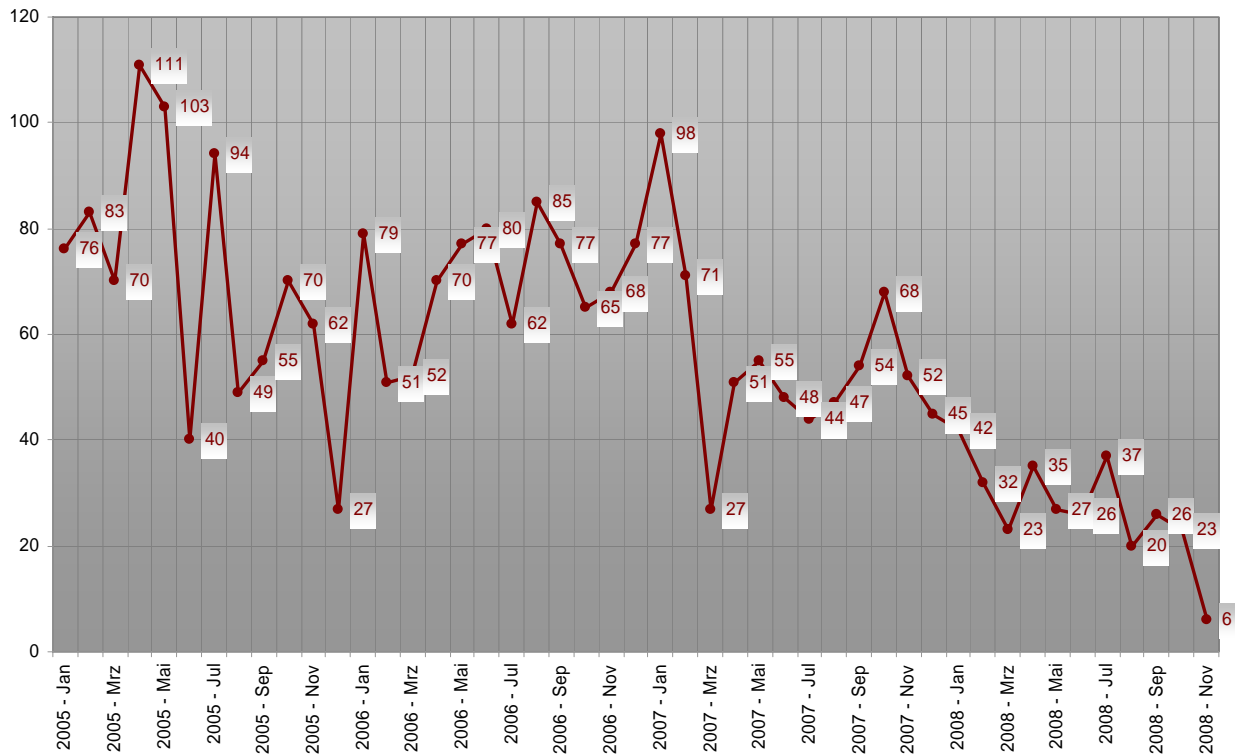




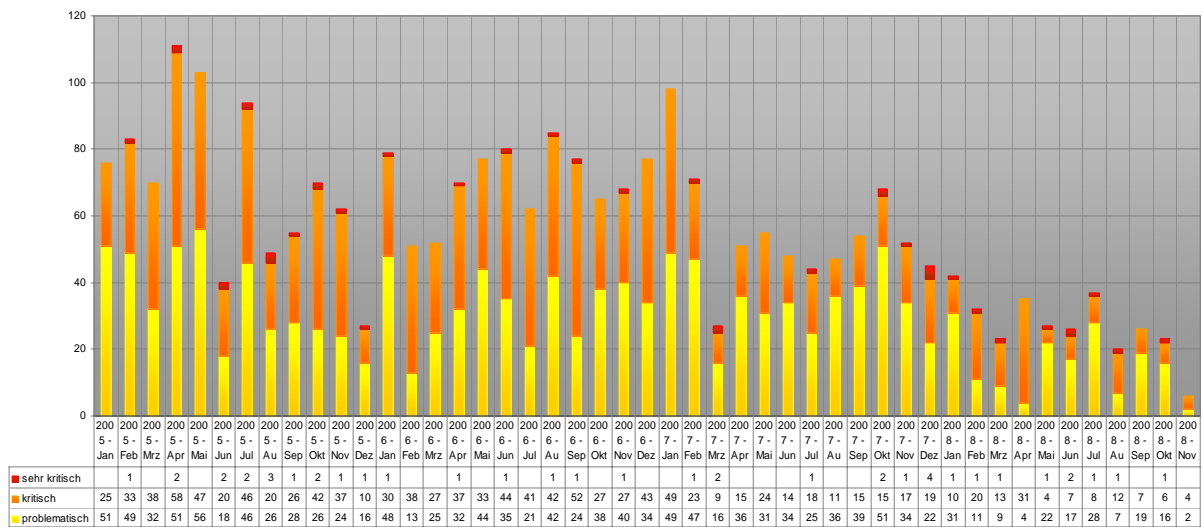
	2008 - Jan	2008 - Feb	2008 - Mrz	2008 - Apr	2008 - Mai	2008 - Jun	2008 - Jul	2008 - Aug	2008 - Sep	2008 - Okt	2008 - Nov	2008 - Dez
◆ Cross Site Scripting (XSS)	4	1	3	2	3	1	5	1	1	2		
◆ Denial of Service (DoS)	9	3	1	1	6	3	6	3	3			
▲ Designfehler	1	7		6	3	6	10	2	3	1	2	
✕ Directory Traversal												
✖ 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	15	4	
✕ 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

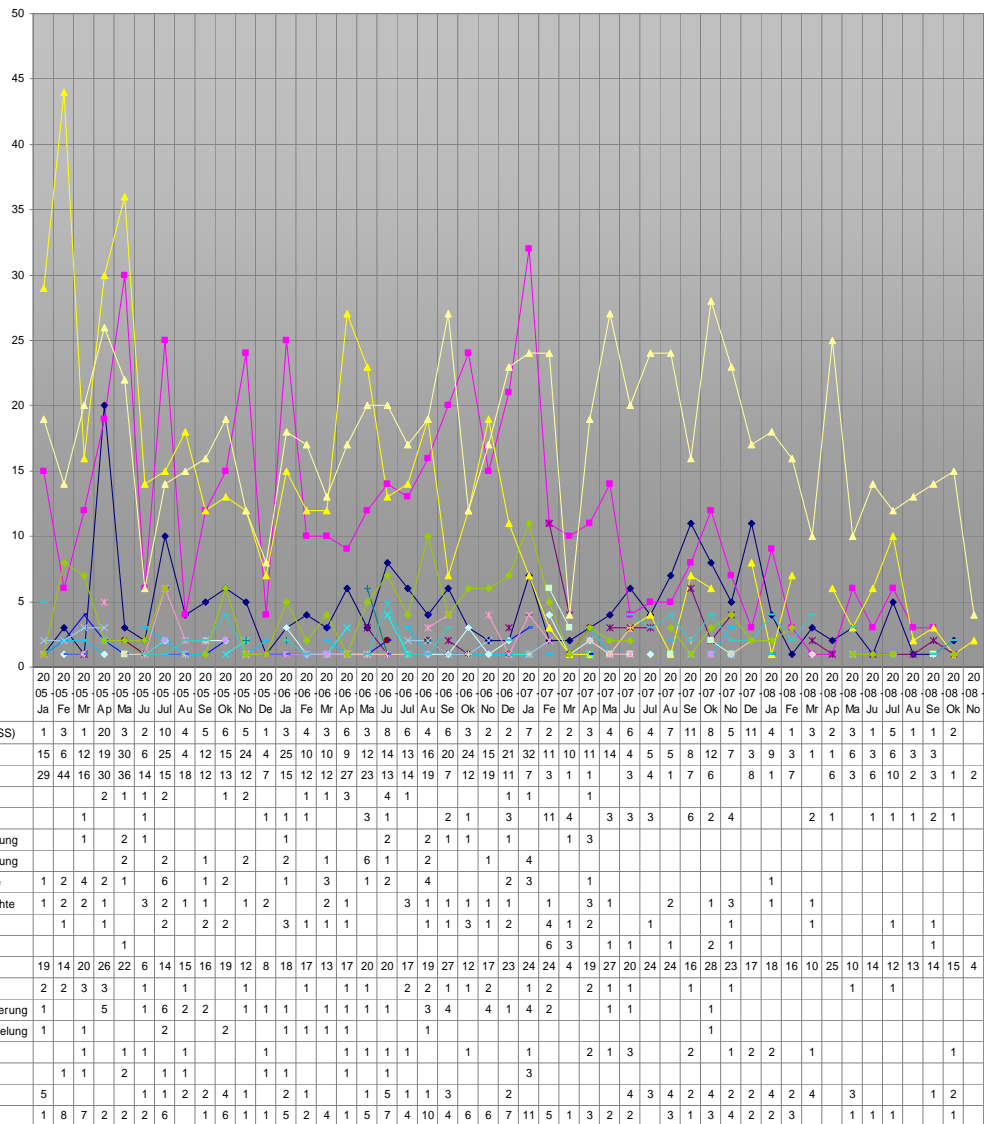
Registrierte Schwachstellen by scip AG



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		
3 (engl.)	2 Buchstaben (engl.)	3 Buchstaben (engl.)

LÖSUNGSWORT

scip monthly Security Summary 19.11.2008

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 **15.12.2008**. 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!](#)