

## Contents

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

### 1. Editorial

#### Kennzahlen und IT-Security?

Gerne stellen wir Menschen unsere Leistungen oder Errungenschaften in Kontrast zu Verdiensten und Achievements anderer Individuen. Unternehmen werden von Menschen gegründet, etabliert und geführt. Daher ist es nicht verwunderlich, dass die Eigenschaft des Vergleichs in die Wirtschaftswelt eingeflossen ist. Der Vergleich gilt dabei als Messlatte und kann externen Stellen, unter anderem, die Stärken oder aber auch Schwächen eines Unternehmens aufzeigen.

Die Herausforderung einer Gegenüberstellung ist das Vergleichen zweier gleichartiger Mengen und dem dabei angewandten Blickwinkel. Ein Vergleich zwischen Apfel und Birne kann mit dem Blickwinkel eines Kosten pro Gramm Gleichnisses Sinn machen. Ein Vergleich zwischen Apfel und Birne hinsichtlich Geschmacks ist jedoch sinnlos, denn die Bewertung dessen ist rein subjektiver Art dem Tester überlassen und kann nicht fundiert dargelegt werden.

Da das Leben meist mehrdimensionale Abstrakte

hervorbringt, musste ein System zur Vereinheitlichung und Simplifizierung entwickelt werden. Eine dieser Massnahmen ist die Verwendung von Kennzahlen. Basierend auf Messtheorien werden dadurch Zahlen ausgegeben, welche im Kennzahlensystem untereinander verglichen werden können. Auch Balanced Score Cards sind ein Kennzahlen basierendes Gebilde.

Die IT-Security ist ein junges Genre. Aufgrund der Tatsache, dass der Information Security ein immer grösserer Stellenwert innerhalb der Unternehmen zugeordnet wird, sind Vergleiche und Entscheidungsgrundlagen basierend auf dem Kennzahlensystem ein vielfach gewünschter Punkt. Vor allem Entscheidungsträger auf höchster Ebene verlangen Entscheidungsgrundlagen in für sie gewohnter Form präsentiert.

Wenden wir uns nun der realen Umsetzung zu und beginnen wir mal mit der ersten Frage: Welche Strategie verfolgt Ihre Security und welche Bereiche gilt es abzudecken? Oder einfacher gesagt, was will man wissen respektive was muss von Gesetztes wegen erkannt werden? Für welche Ebene sind die Kennzahlen zu erheben?



Bevor wir nun diese Frage auf der Papierebene zu lösen beginnen, schauen wir mal ein paar Schritte im Prozess voraus. Irgendwo müssen wir bestimmt Daten sammeln, schlussendlich müssen wir ja eine Erfassung der Grunddaten (automatisiert) umsetzen. Da stellt sich die Frage: Offerieren die für uns relevanten Systeme und Applikationen überhaupt brauchbare Datensätze? [scip 2005] Wie sieht es mit deren Aussagekraft aus? Wie sind diese Daten gegen Manipulationen geschützt? Etc.

Ich bin persönlich der Meinung, dass die Einführung eines Kennzahlensystems etwas Sinnvolles ist und die IT- als auch die Information Security einen grossen Schritt vorwärts bringen wird.

Zur effektiven Umsetzung eines Kennzahlensystems innerhalb der Information Security reicht

weder der vielgepredigte Top-Down noch der inverse Bottom-Up Approach. Sowohl auf Management Ebene als auch auf technischer Ebene fehlen die Grundlagen zur Etablierung eines integralen und umfassenden Kennzahlensystems. Mir ist nicht bekannt wie lange es gedauert hat, um für die Finanzwelt ein einigermaßen funktionierendes System zu entwickeln. Für das junge Genre der Information Security ist noch ein grosser Teil des Weges zu beschreiten.

Ein mögliches und bereits praktiziertes Vorgehen ist der Beginn der Etablierung eines reduzierten Kennzahlensystems auf der Ebene einzelner Unternehmungen respektive Geschäftsbereiche. Dabei können in einer definierten homogenen Umgebung Erfahrungen gesammelt und gleichzeitig die ersten verdichteten Zahlen übergeben werden. Ein enorm wichtiger Nebeneffekt dieses Vorgehens sind die automatisch auftauchenden neuen Anforderungen der zahlenden Kundschaft an die entsprechenden Lieferanten und Softwarehersteller.

*"Wenn sich etwas nicht mit Bildern erklären lässt, ist es keine Wissenschaft, sondern blosser Meinung. Man weiss schon lange, dass ein Pferd schneller läuft als das andere - aber welches? Der Unterschied ist entscheidend." - Robert A. Heinlein 1973*

Simon Zumstein <sizu-at-scip.ch>  
Geschäftsleiter  
Zürich, 17. Oktober 2005

## 2. scip AG Informationen

### 2.1 Nachrichtensendung 10 vor 10



Das Nachrichtenformat 10 vor 10 des staatlichen schweizerischen Fernsehens SFDRS (<http://www.sfdrs.ch>), vergleichbar mit dem Heute Journal des ZDF (<http://www.zdf.de>), sendete

am Dienstag dem 4. Oktober 2005 einen Beitrag über Datendiebstahl durch Internet-Kriminelle bei Firmen.

Die scip AG wurde dazu in ihrer Tätigkeit als renommierter Auftragsangreifer aus dem Internet für Grossfirmen und Finanzinstitute befragt. Als Spezialist für Computersicherheit wurde Herr Marc Ruet in den Büroräumlichkeiten der scip AG interviewt.

### 2.2 Computerworld

Marc Ruet beantwortet in der aktuellen Ausgabe der Computerworld vom 14. Oktober 2005 (<http://www.computerworld.ch>) Fragen bezüglich der Sicherheit von Online-Banking.



Den Artikel finden Sie online als PDF unter <http://www.computec.ch/download.php?view.687>

### 2.3 computec.ch

computec.ch besteht seit 1997 und ist DAS werbefreie und deutschsprachige Online-Archiv für Publikationen zu den Themen Computer, Technik und Sicherheit.



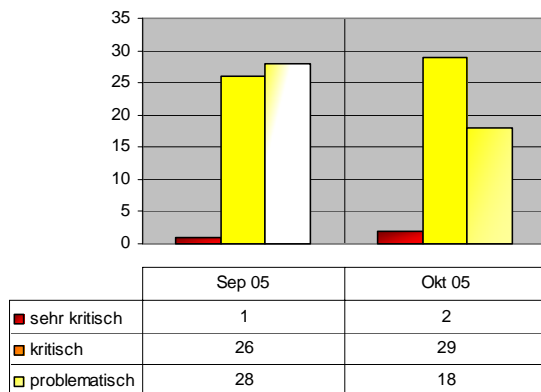
Die aktuelle Version 2.0, welche seit dem 16. Oktober 2005 aufgeschaltet ist, verheisst vor allem ein Mehr an Interaktivität für den Benutzer. Marc Ruet hat das Content Management System (CMS) einmal mehr optimiert und wichtige Features addiert.

Besuchen Sie <http://www.computec.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:

- 3.1 Mozilla Thunderbird bis 1.0.6 HTML sourcetext-Tag Denial of Service
- 3.2 Mozilla Firefox bis 1.5 Beta 2 HTML sourcetext-Tag Denial of Service
- 3.3 Oracle verschiedene Produkte 85 verschiedene Sicherheitslücken
- 3.4 Snort bis 2.4.3 Back Orifice Pre-Processor Pufferüberlauf
- 3.5 ISC Lynx bis 2.8.6dev.13 HTrjis() NNTP-Header Pufferüberlauf
- 3.6 McAfee GroupShield bis 4.4.0 korrupte ARJ-Archive Scanning umgehen
- 3.7 Veritas NetBackup bis 6.0 bpjava-msvc COMMAND\_LOGON\_TO\_MSERVER-Kommando Format String
- 3.8 Symantec Brightmail AntiSpam bis 6.0.2 MIME-Verarbeitung bmsvr Denial of Service
- 3.9 Sun Java System Application Server 7.x JSP-Quelltext erweiterte Leserechte
- 3.10 Microsoft Windows 2000, XP und Server 2003 Client Service for NetWare Pufferüberlauf
- 3.11 Microsoft Windows 2000, XP und Server 2003 Transaction Internet Protocol Denial of Service
- 3.12 Microsoft Windows 2000, XP und Server 2003 COM+ korrupte Netzwerk-Nachricht

#### Pufferüberlauf

- 3.13 Microsoft Windows 2000, XP und Server 2003 Microsoft Distributed Transaction Coordinator Pufferüberlauf
- 3.14 Microsoft DirectX 8.0 bis 9.0c unbekannter Pufferüberlauf
- 3.15 Microsoft Internet Explorer bis 6.0 FTP Download korrupter Dateiname erweiterte Rechte
- 3.16 Microsoft Windows 2000, XP und Server 2003 Explorer HTML-Vorschau Cross Site Scripting
- 3.17 Microsoft Windows 2000, XP und Server 2003 korrupte Ink-Datei Pufferüberlauf
- 3.18 Microsoft Windows 2000, XP und Server 2003 korrupte Ink-Datei Programmcode ausführen
- 3.19 Microsoft Exchange 2000 SMTP Collaboration Data Objects Pufferüberlauf
- 3.20 Microsoft Windows 2000, XP und Server 2003 Plug-and-Play Dienst Pufferüberlauf
- 3.21 BEA WebLogic 24 verschiedene Schwachstellen
- 3.22 RarLabs WinRAR bis 3.50 UNACEV2.DLL korruptes ACE-Archiv langer Dateiname Pufferüberlauf
- 3.23 Sun Java System Directory Server bis 5.2 HTTP Admin-Interface erweiterte Rechte
- 3.24 Mozilla Firefox bis 1.0.7 HTML iframe-Tag lange Attribute Pufferüberlauf
- 3.25 Citrix MetaFrame Presentation Server 3.0 und 4.0 Richtlinie anderer Hostname umgehen
- 3.26 RealNetworks RealPlayer bis 10.0.5.756 Fehlermeldung Format String
- 3.27 Mozilla Firefox bis 1.0.7 Fenster öffnen erweiterte Rechte
- 3.28 Mozilla Firefox bis 1.0.7 XMLHttpRequest erweiterte Rechte
- 3.29 Mozilla Firefox bis 1.0.7 Unicode zero-width non-joiner Pufferüberlauf
- 3.30 Mozilla Firefox bis 1.0.7 korrupte XBM-Bilder Pufferüberlauf

#### 3.1 Mozilla Thunderbird bis 1.0.6 HTML sourcetext-Tag Denial of Service

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 17.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1828>

Das Mozilla-Projekt versucht eine open-source Suite - hauptsächlich bestehend aus

Webbrowser und Mailclient - zur Verfügung zu stellen. Auf whitedust.net wurde auf eine Denial of Service-Schwachstelle hingewiesen, die den Mailclient Thunderbird bis 1.0.6 betrifft. Und zwar friert dieser - ebenso wie Mozilla Firefox - ein, wenn der sourcetext-Tag in bestimmter Konstellation (besonders Verschachtelungen mit anderen Tags) genutzt wird. Als Proof-of-Concept wurde die Zeile `[html][body][strong]scip.ch[sourcetext][body][html]` mitpubliziert. Der Fehler, er generiert eine CPU-Auslastung von 100 %, wird voraussichtlich in der kommenden Software-Version behoben.

#### Expertenmeinung:

Mozilla Firefox gilt als ernstzunehmende und sichere Alternative zum Branchenriesen Microsoft Internet Explorer. In vielen der letzten Meldungen zu Schwachstellen im Internet Explorer wird darauf verwiesen, endlich auf eine Lösung wie Firefox umzusteigen. Dieses Mehr an Popularität hat aber kurzfristig auch dem Firefox-Projekt zusätzliche Angriffsfläche beschert. Noch nie wurden innerhalb so kurzer Zeit so viele ernstzunehmende Sicherheitslücken in Mozilla Firefox bekannt. Die alte Fausregel, dass zusätzliche Popularität eines Produkts die meisten Sicherheitslücken in diesem zu Tage fördern wird, hat sich also einmal mehr bewahrheitet.

### 3.2 Mozilla Firefox bis 1.5 Beta 2 HTML sourcetext-Tag Denial of Service

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 17.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1827>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, wobei das aktuelle Ziel der Entwickler ein Marktanteil von 10 % darstellt. Auf whitedust.net wurde auf eine Denial of Service-Schwachstelle hingewiesen, die den Mozilla Firefox bis 1.5 Beta 2 betrifft. Und zwar friert dieser ein, wenn der sourcetext-Tag in bestimmter Konstellation (besonders Verschachtelungen mit anderen Tags) genutzt wird. Als Proof-of-Concept wurde die Zeile `[html][body][strong]scip.ch[sourcetext][body][html]` mitpubliziert. Der Fehler, er generiert eine CPU-Auslastung von 100 %, wurde schon in der Beta 2 der Version 1.5 des Webbrowsers behoben.

#### Expertenmeinung:

Mozilla Firefox gilt als ernstzunehmende und sichere Alternative zum Branchenriesen Microsoft Internet Explorer. In vielen der letzten Meldungen zu Schwachstellen im Internet Explorer wird darauf verwiesen, endlich auf eine Lösung wie Firefox umzusteigen. Dieses Mehr an Popularität hat aber kurzfristig auch dem Firefox-Projekt zusätzliche Angriffsfläche beschert. Noch nie wurden innerhalb so kurzer Zeit so viele ernstzunehmende Sicherheitslücken in Mozilla Firefox bekannt. Die alte Fausregel, dass zusätzliche Popularität eines Produkts die meisten Sicherheitslücken in diesem zu Tage fördern wird, hat sich also einmal mehr bewahrheitet.

### 3.3 Oracle verschiedene Produkte 85 verschiedene Sicherheitslücken

Einstufung: **sehr kritisch**  
 Remote: Teilweise  
 Datum: 18.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1826>

Oracle ist eine vor allem im professionellen Umfeld gern eingesetzte Datenbank-Lösung. Oracle gab im Rahmen seines vierteljährlichen Critical Patch Update ein Advisory heraus, das sich 85 verschiedenen - teilweise kritischen - Sicherheitslücken annimmt. Das HTML-Dokument weist in einer Matrix die Schwachstellen aus, zeigt mitunter auch ihre Auswirkungen und Voraussetzung auf. Es ist jedoch nicht ersichtlich, welcher Kategorie (z.B. Pufferüberlauf oder Format String) die jeweiligen Fehler zugeordnet werden müssen. Technische Details oder Exploits zur Schwachstelle sind bisher nicht bekannt, könnten jedoch in den kommenden Tagen auf den einschlägigen Sicherheitsmailinglisten und -Webseiten folgen. Oracle hat entsprechend Patches für die betroffenen Produkte bereitgestellt.

#### Expertenmeinung:

Wahrhaftig eine Vielzahl an Schwachstellen, die Oracle hier vier Mal im Jahr zusammenträgt. Für Administratoren entsprechender Lösungen ist dies natürlich sodann eine stressige Zeit, in der die jüngsten Patches überprüft und eingespielt werden sollen. Gut und gerne mindestens eine Woche ist man damit beschäftigt, sich auf ein solches Patching - und wir reden hier nur von einem System - vorzubereiten. Überstunden sind deshalb die Regel. Ob dieses Patchday-Prinzip, wie es auch Microsoft umzusetzen pflegt, wirklich so von Vorteil ist, muss nach wie vor bezweifelt werden.

### 3.4 Snort bis 2.4.3 Back Orifice Pre-Processor Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 18.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1825>

Snort ist eine beliebte, netzwerkbasierende open-source Intrusion Detection-Lösung. Neel Mehta der ISS X-Force entdeckte, dass der Pre-Processor für Back Orifice in Snort bis 2.4.3 gegen eine Pufferüberlauf-Angriffe verwundbar ist. Ein Angreifer kann durch den manipulativen Datenverkehr beliebigen Programmcode auf dem Snort-System, das die Überwachung umsetzt, ausführen lassen. Das Problem ist vor allem deswegen kritisch, da eine Kompromittierung des Snort-Rechners auch dann stattfindet, wenn der Angriff nicht auf ihn gerichtet wird - Wenn stattdessen ein Host in einem überwachten Segment zum Ziel wird. Es sind bisher keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler wurde in der aktuellen Snort-Version 2.4.3 behoben. Als Workaround wird empfohlen, auf die Netzwerküberwachung auf Back Orifice zu verzichten. Dieser wird ind er heutigen Zeit nur sehr selten eingesetzt, da seine hohe Bekanntheit dafür sorgte, dass praktisch alle Antiviren-Lösungen das Produkt erkennen können.

#### Expertenmeinung:

Diese Schwachstelle ist sehr kritisch, denn ohne viel Aufwand lässt sich über das Netzwerk Programmcode auf dem Snort-Sensor ausführen. Da Snort aufgrund seiner vielen Vorteile so manchem kommerziellen NIDS vorgezogen wird, werden viele Netzwerke von dieser Schwachstelle betroffen sein. Entsprechende Exploit-Beispiele werden aufgrund der hohen Verbreitung von Snort sicher in den kommenden Tagen folgen.

### 3.5 ISC Lynx bis 2.8.6dev.13 HTrjis() NNTP-Header Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 17.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1815>

Lynx ist ein textbasierter Webbrowser der unter Unix entwickelt wurde, mittlerweile aber für fast alle Betriebssysteme verfügbar ist. Er wird vorwiegend nur noch durch Puristen eingesetzt. Ulf Harnhammar des Debian Security Audit

Project entdeckte eine Pufferüberlauf-Schwachstelle in ISC Lynx bis 2.8.6dev.13. Diese kann durch einen korrupten Header einer NNTP-Verbindung provoziert werden. Der Finder stellt mit `nntp://malicious.server/group.name` eben eine korrupte Newsgroup zur Verfügung, unter der man die Verwundbarkeit von Lynx überprüfen kann. ISC wurde frühzeitig über das Problem informiert und hat mit einer aktualisierten Software-Version reagiert.

#### Expertenmeinung:

Diese Schwachstelle ist interessant und zeigt, dass auch normale Client-Software für indirekte Angriffe genutzt werden kann. Umso erschreckender ist, dass dieser Pufferüberlauf so einfach herbeigeführt werden kann. Dies ist eindeutig auf Unachtsamkeit von Seiten der Software-Entwickler zurückzuführen. In sicherheitsrelevanten Umgebungen sollte man so oder so auf unnötige Software verzichten. Auch wenn es sich um alteingesessene und so schlanke Software wie den Lynx handelt.

### 3.6 McAfee GroupShield bis 4.4.0 korrupte ARJ-Archive Scanning umgehen

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 13.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1810>

Ein Antivirenprogramm (auch Virens Scanner) ist eine Software, die ihr bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspüren, blockieren und gegebenenfalls beseitigen soll. Vorbeugendes Virens scanning und ein automatischer Outbreak Manager von McAfee GroupShield verhindern die Störung des Systems durch böartigen Code. fRoGGz der SecuBox Labs entdeckte ein Problem, das eine Vielzahl an Antiviren-Lösungen betrifft. So können über korrupte ARJ-Archive die Scanning-Funktionalität umgangen werden. Korrupter Programmcode kann sich so ohne frühzeitige Entdeckung oder Entfernung verbreiten. Es sind keine exakten technischen Details oder ein Exploit bekannt. Als Workaround wird empfohlen, die betroffenen Archive schon frühzeitig mit einem umfassenden Gateway-Mechanismus abzufangen und zu entpacken, um die Umgehung zu verhindern.

#### Expertenmeinung:

Dies ist einmal mehr ein flächendeckendes Problem, das eine Vielzahl der verschiedenen Antiviren-Lösungen betrifft. Es ist schon

immerwieder erstunlich, dass derlei Probleme bei so vielen Produkten gegeben sind und kein Hersteller Anstalten unternahm, um sie zu verhindern. So liegt es nun an den Firmen selbst, schnellstmöglich Gegenmassnahmen umzusetzen, bis die Antiviren-Firmen Patches oder aktualisierte Software-Versionen zur Verfügung stellen.

### 3.7 Veritas NetBackup bis 6.0 bjava-msvc COMMAND\_LOGON\_TO\_MSERV ER-Kommando Format String

Einstufung: **kritisch**  
Remote: Ja  
Datum: 13.10.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1806>

Veritas stellt neben dem Cluster Server für die Lastverteilung bzw. Leistungskombinierung ebenfalls eine Backup-Lösung zur Verfügung. Der Hersteller meldet einmal mehr einen Fehler bei der Administration über das Java-GUI. So existiert eine Format String-Schwachstelle bei der Verarbeitung des COMMAND\_LOGON\_TO\_MSERV-Kommandos. Darüber kann ein Angreifer erweiterte Rechte erlangen. Es sind keine weiteren technischen Details oder ein Exploit zur Schwachstelle bekannt. Veritas hat einen Patch zum Problem herausgegeben.

#### Expertenmeinung:

Eine der wenigen Format String Attacks dieses Jahres. Trotzdem zeigt sie sehr imposant, wie wirkungsvoll diese Angriffsart sein kann. Es ist nur eine Frage der Zeit, bis ein Exploit auf SecuriTeam.com und vergleichbaren Seiten publiziert werden wird.

### 3.8 Symantec Brightmail AntiSpam bis 6.0.2 MIME-Verarbeitung bmserv Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 12.10.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1805>

Symantec Brightmail AntiSpam bietet wirkungsvolle Spam-Erkennung mit einer hohen Genauigkeitsrate, bei der Fehlerkennungen verhindert werden. Diese preisgekrönte Antispam-Lösung schützt nicht nur weitgehend vor Spam-Angriffen in Echtzeit, sondern erkennt auch aktiv erstmalige Spam-E-Mails. Wie der

Hersteller meldet, existiert ein Denial of Service-Problem in den Versionen bis 6.0.3. Durch den Fehler in der MIME-Verarbeitung kann der bmserv zum Absturz gebracht werden. Es sind keine weiteren Details oder ein Exploit zur Schwachstelle bekannt. Symantec hat für die Versionen 6.0.1 und 6.0.2 dedizierte Patches bereitgestellt.

#### Expertenmeinung:

Die Entwickler von Mail- und Spam-Lösungen nehmen es nicht immer so genau, wenn es um die Netzwerksicherheit geht. Besonders in Unternehmen kann es ärgerlich sein, wenn ein verärgerter oder gelangweilter Mitarbeiter ständig die Antiviren-Lösung abschießt. Daher unbedingt die aktuelle Software-Version installieren.

### 3.9 Sun Java System Application Server 7.x JSP-Quelltext erweiterte Leserechte

Einstufung: **kritisch**  
Remote: Ja  
Datum: 13.10.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1804>

Der Sun Java System Application Server ist eine kommerzielle Webserver-Lösung von Sun Microsystems Inc. Wie der Hersteller knapp bekannt gab, existiert ein Problem in der 7er-Reihe. Durch dieses könne ein Angreifer die Inhalte der JSP-Quellen lesen. Es sind keine Details oder ein Exploit zur Schwachstelle bekannt. Sun hat den Fehler mit Patches adressiert.

#### Expertenmeinung:

Da nahezu keine Details zur Schwachstelle bekannt sind, ist die Einschätzung sehr schwierig und zum jetzigen Zeitpunkt nicht möglich. Gerade deshalb bleibt Administratoren nichts anderes übrig, als schnellstmöglich die empfohlenen Gegenmassnahmen umzusetzen.

### 3.10 Microsoft Windows 2000, XP und Server 2003 Client Service for NetWare Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 11.10.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1801>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des



professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-046 wird festgehalten, dass eine Pufferüberlauf-Schwachstelle im Client Service for NetWare existiert. Ein Angreifer kann so beliebigen Programmcode ausführen. Abgesehen von Microsoft Windows Server 2003 mit Service Pack 1 ist das auch ohne authentisierten Benutzer möglich. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Dieses Problem könnte durchaus zu einem Renner bei Angreifern werden, wenn ein handlicher Exploit herausgegeben wird. Das Ausbleiben eines absoluten Horror-Szenarios ist deshalb gegeben, da "nur" Windows 2000 sowie Windows XP unter gewissen Umständen betroffen sind. Dies soll aber nicht über die Gefahr hinwegtäuschen, die in derlei Umgebungen zu finden ist.

### 3.11 Microsoft Windows 2000, XP und Server 2003 Transaction Internet Protocol Denial of Service

Einstufung: **kritisch**

Remote: Ja

Datum: 11.10.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1798>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-051 werden einige kritische Schwachstellen, die eben diese Systeme betreffen. Eine davon schlägt sich in einer Denial of Service-Schwachstelle in MSDTC (Microsoft Distributed Transaction Coordinator) nieder. Unterstützt dieser TIP (Transaction Internet Protocol), kann eine Denial of Service-Attacke umgesetzt werden, die sowohl den Client als auch den Server der Verbindung affektieren kann. Bisher sind keine Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Sobald ein Exploit zu dieser Schwachstelle bekannt wird, wird der Fehler in Skript-Kiddie Kreisen eine hohe Verbreitung erreichen. Es ist zwar nicht damit zu rechnen, dass die Popularität der Schwachstelle das Ausmass eines WinNuke95 oder SMBdie/SMBkill erlangen wird - Die Popularität einschränken wird die

erforderliche und nicht standardmässig angebotene TIP-Unterstützung. Glücklicherweise handelt es sich zudem um eine Denial of Service-Schwachstelle, bei der keine erweiterten Rechte erzwungen werden können. Wäre dies der Fall gewesen, hätte eine weitere Katastrophe ähnlich der W32.Blaster.Worm auf uns zusteuern können.

### 3.12 Microsoft Windows 2000, XP und Server 2003 COM+ korrupte Netzwerk-Nachricht Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 11.10.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1797>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-051 werden einige kritische Schwachstellen, die eben diese Systeme betreffen. Eine davon schlägt sich in einem Pufferüberlauf COM+ nieder. Durch eine korrupte Netzwerk-Nachricht kann sodann ein Angreifer beliebigen Programmcode ausführen lassen. Vom Problem betroffen sind Microsoft Windows 2000 und Server 2003 sowie XP. Bei Windows Server 2003 sowie XP mit SP1/SP2 kann der Angriff jedoch nur lokal umgesetzt werden. Bisher sind keine Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Dieses Problem könnte durchaus zu einem Renner bei Angreifern werden, wenn ein handlicher Exploit herausgegeben wird. Das Ausbleiben eines absoluten Horror-Szenarios ist deshalb gegeben, da "nur" Windows 2000 sowie Windows XP samt Server 2003 betroffen sind, detaillierte technische Hintergrundinformationen und Exploits bisher fehlen. Dies soll aber nicht über die Gefahr hinwegtäuschen, die in derlei Umgebungen zu finden ist.

### 3.13 Microsoft Windows 2000, XP und Server 2003 Microsoft Distributed Transaction Coordinator Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 11.10.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1796>



Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-051 werden einige kritische Schwachstellen, die eben diese Systeme betreffen. Eine davon schlägt sich in einem Pufferüberlauf im Microsoft Distributed Transaction Coordinator nieder. Dadurch kann ein Angreifer beliebigen Programmcode ausführen lassen. Vom Problem betroffen sind Microsoft Windows 2000 und Server 2003 sowie XP mit Service Pack 1 (SP2 ist nicht betroffen). Bisher sind keine Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Dieses Problem könnte durchaus zu einem Renner bei Angreifern werden, wenn ein handlicher Exploit herausgegeben wird. Das Ausbleiben eines absoluten Horror-Szenarios ist deshalb gegeben, da "nur" Windows 2000 sowie Windows XP samt Server 2003 betroffen sind, detaillierte technische Hintergrundinformationen und Exploits bisher fehlen. Dies soll aber nicht über die Gefahr hinwegtäuschen, die in derlei Umgebungen zu finden ist.

### 3.14 Microsoft DirectX 8.0 bis 9.0c unbekannter Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 11.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1795>

DirectX ist eine Sammlung von Application Programming Interfaces (APIs) für Multimediaprogramme auf der Windows-Plattform. Diese wurde mit Microsoft Windows 95 eingeführt und wird vorzugsweise zur Darstellung komplexer 2d- und 3d-Grafiken (z.B. in Spielen) genutzt. Im Microsoft Security Bulletin MS05-050 ist nachzulesen, dass ein nicht näher spezifizierter Pufferüberlauf in Microsoft DirectX 8.0 bis 9.0c existiert. Ein Angreifer könne durch die korrupte Nutzung der API beliebigen Programmcode ausführen. Bisher sind keine weiteren Details oder ein Exploit zum Fehler bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht. Es wird in hochsicheren Umgebungen, die nicht auf DirectX angewiesen sind (z.B. im Server-Bereich), empfohlen, auf die Installation von DirectX zu verzichten.

#### Expertenmeinung:

Eine der ernstzunehmenden Sicherheitslücken, die durch den jüngsten Patchday von Microsoft behoben werden kann. Zum Glück sind keine Details bekannt, wie diese Schwachstelle ausgenutzt werden kann, denn sonst würde dieser Angriff für eine Vielzahl der Angreifer sehr interessant werden. Umso dringender ist es, die neuesten Bugfixes zu installieren.

### 3.15 Microsoft Internet Explorer bis 6.0 FTP Download korrupter Dateiname erweiterte Rechte

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 11.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1794>

Der Microsoft Internet Explorer, abgekürzt MSIE oder IEX, ist einer der am meisten verbreiteten Webbrowser. Seine Verbreitung wird zur Zeit auf etwa 95 % geschätzt, was sicher auch damit zu tun hat, das er ein Bestandteil moderner Windows-Betriebssysteme ist und somit auf diesen ein Quasi-Standard für Webbrowsing darstellt. Im Microsoft Security Bulletin MS05-044 wird auf einen Fehler im Microsoft Internet Explorer bis 6.0 hingewiesen. Durch einen korrupten Dateinamen kann während eines FTP-Downloads erweiterte Rechte erlangt - andere Dateien überschrieben - werden. Bisher sind keine weiteren Details oder ein Exploit zum Fehler bekannt. Diese Schwachstelle könnte mit derjenigen, die in scipID 1091 besprochen wird, verknüpft sein. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Dies ist eine sehr interessante Schwachstelle, von der sehr wahrscheinlich auch noch andere FTP-Clients betroffen sind. Die Zukunft wird zeigen, welche Tragweite derlei Sicherheitslücken haben werden. Das potentielle Risiko ist jedoch durchaus hoch, weshalb Gegenmassnahmen nicht hinausgezögert werden sollten.

### 3.16 Microsoft Windows 2000, XP und Server 2003 Explorer HTML-Vorschau Cross Site Scripting

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 11.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1793>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-049 werden drei Schwachstellen festgehalten, die in Bezug auf die Dateibehandlung gegeben ist. Eine davon betrifft die HTML-Vorschau des Explorers. Dieser hat Mühe beim Anzeigen gewisser Zeichen, was für eine Script-Injection erhalten kann. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Diese Sicherheitslücke ist scheint kritisch, wobei man jedoch von Glück sprechen kann, dass das Problem nur lokal ausnutzbar ist und zur Zeit noch Details fehlen. Trotzdem sollte man sich schnellstmöglich bemühen, das eigene System entsprechend abzusichern. Es ist nämlich soweit nicht bekannt, inwieweit sich diese Schwachstelle zum Beispiel über einen Webbrowser initiieren lässt (z.B. Ein semi-automatischer Datei-Download).

### 3.17 Microsoft Windows 2000, XP und Server 2003 korrupte Ink-Datei Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 11.10.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1792>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-049 werden drei Schwachstellen festgehalten, die in Bezug auf die Dateibehandlung gegeben ist. Eine davon betrifft die Möglichkeit, dass über korrupte Ink-Dateien Programmcode mit der Hilfe eines Pufferüberlaufs ausgeführt werden kann. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Diese Sicherheitslücke ist scheint kritisch, wobei man jedoch von Glück sprechen kann, dass das Problem nur lokal ausnutzbar ist und zur Zeit noch Details fehlen. Trotzdem sollte man sich schnellstmöglich bemühen, das eigene System entsprechend abzusichern. Es ist nämlich soweit nicht bekannt, inwieweit sich diese Schwachstelle zum Beispiel über einen

Webbrowser initiieren lässt (z.B. Ein semi-automatischer Datei-Download).

### 3.18 Microsoft Windows 2000, XP und Server 2003 korrupte Ink-Datei Programmcode ausführen

Einstufung: **kritisch**  
Remote: Ja  
Datum: 11.10.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1791>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-049 werden drei Schwachstellen festgehalten, die in Bezug auf die Dateibehandlung gegeben ist. Eine davon betrifft die Möglichkeit, dass über korrupte Ink-Dateien Programmcode mit den Rechten des Benutzers ausgeführt werden kann, der auf diesen Link zurückgreift. Bisher sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Diese Sicherheitslücke ist scheint kritisch, wobei man jedoch von Glück sprechen kann, dass das Problem nur lokal ausnutzbar ist und zur Zeit noch Details fehlen. Trotzdem sollte man sich schnellstmöglich bemühen, das eigene System entsprechend abzusichern. Es ist nämlich soweit nicht bekannt, inwieweit sich diese Schwachstelle zum Beispiel über einen Webbrowser initiieren lässt (z.B. Ein semi-automatischer Datei-Download).

### 3.19 Microsoft Exchange 2000 SMTP Collaboration Data Objects Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 11.10.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1790>

Microsoft Exchange 2000 ist ein von vielen Unternehmen gern eingesetzter Mailserver, der jedoch an einigen Stellen schon durch die Version 2003 abgelöst wurde. Wie Microsoft im Security Bulletin MS05-048 festhält, existiert in Microsoft Exchange 2000 auf Microsoft Windows 2000 ein ernstzunehmendes Problem in Bezug auf SMTP-Verkehr (Email). Über einen Pufferüberlauf-Fehler in Collaboration Data

Objects (CDO) kann ein Angreifer mit einer korrupten Email beliebigen Programmcode ausführen lassen. Technische Details oder ein Exploit zur Schwachstelle sind noch nicht bekannt. Microsoft hat im Rahmen des Patchdays einen entsprechenden Patch herausgebracht.

#### Expertenmeinung:

Dieses Problem könnte durchaus zu einem Renner bei Angreifern werden, wenn ein Exploit herausgegeben wird. Man kann von Glück sprechen, dass in der Tat Exchange 2000 mittlerweile durch die 2003er Version abgelöst wurde. In Umgebungen, in denen dieser Schritt noch nicht gemacht wurde, wird das Einspielen des jüngsten Patches unabdingbar.

### 3.20 Microsoft Windows 2000, XP und Server 2003 Plug-and-Play Dienst Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 11.10.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1789>

Die beiden Betriebssysteme Microsoft Windows 2000 und XP sind eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Im Microsoft Security Bulletin MS05-047 ist nachzulesen, dass der Plug-and-Play Dienst eine Pufferüberlauf-Schwachstelle aufweist. Bei Windows 2000 und XP mit Service Pack 1 kann ein nicht-authentisierter Benutzer beliebigen Programmcode ausführen lassen. Bei Windows XP mit Service Pack 2 hingegen ist eine vorgängige Authentisierung erforderlich. Bisher sind keine technischen Details oder Exploits zur Schwachstelle bekannt. Als Workaround listet Microsoft auf, dass Verbindungen zu den NetBIOS-Ports (tcp/139 und 445) unterbunden werden sollten. Dies kann mit der hauseigenen Internetverbindungsfirewall, einer dedizierten Desktop Firewall oder einer autonomen Firewall-Lösung geschehen.

#### Expertenmeinung:

Dieses Problem könnte durchaus zu einem Renner bei Angreifern werden, wenn ein handlicher Exploit herausgegeben wird. Das Ausbleiben eines absoluten Horror-Szenarios ist deshalb gegeben, da "nur" Windows 2000 sowie Windows XP unter gewissen Umständen betroffen sind. Dies soll aber nicht über die Gefahr hinwegtäuschen, die in derlei Umgebungen zu finden ist.

### 3.21 BEA WebLogic 24 verschiedene Schwachstellen

Einstufung: **sehr kritisch**

Remote: Teilweise

Datum: 11.10.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1787>

BEA Weblogic Server erhöhen die Produktivität und senken die Kosten der IT-Abteilungen, indem er eine einheitliche, vereinfachte und erweiterbare Architektur bietet. BEA Weblogic Server basiert auf Applikationsinfrastruktur-Technologien von BEA Produkten, die weltweit von tausenden Kunden erfolgreich eingesetzt werden. Gleich 24 Sicherheitslücken hat der Hersteller bekanntgegeben. Zeitgleich wurden auch entsprechende Patches bzw. aktualisierte Versionen der betroffenen Komponenten zur Verfügung gestellt. Zu den meisten Schwachstellen sind keine technischen Details oder Exploits bekannt.

#### Expertenmeinung:

Wahrhaftig eine Vielzahl an Schwachstellen, die hier zusammengetragen worden sind. Für Administratoren entsprechender Lösungen ist dies natürlich sodann eine stressige Zeit, in der die jüngsten Patches überprüft und eingespielt werden sollen - Vor allem, da auch der Patchday von Microsoft diesen Monat umfassend ausfällt. Gut und gerne mindestens eine Woche ist man damit beschäftigt, sich auf ein solches Patching - und wir reden hier nur von einem System - vorzubereiten. Überstunden sind deshalb die Regel. Ob dieses Patchday-Prinzip wirklich so von Vorteil ist, muss nach wie vor bezweifelt werden.

### 3.22 RarLabs WinRar bis 3.50 UNACEV2.DLL korruptes ACE-Archiv langer Dateiname Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 11.10.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1785>

WinRar der Firma RarLabs ist ein Kompressions-Tool, das mit verschiedenen Formaten, in erster Linie RAR und ZIP, zurecht kommt. Das Kernstück wird auch von so mancher Antiviren-Software verwendet, um gepackte Dateien zu entpacken und zu untersuchen. Tan Chew Keong von Secunia Research entdeckte zwei kritische Fehler in WinRar bis 3.50. Einer ist in

der Library UNACEV2.DLL zu suchen. Diese ist in Bezug auf lange Dateinamen innerhalb korrupter ACE-Archive auf eine Pufferüberlauf-Attacke anfällig. Darüber liesse sich beliebiger Programmcode ausführen. Es sind bisher keine technischen Details oder ein Exploit zur Schwachstelle bekannt. RarLabs wurde frühzeitig von Secunia über das Problem informiert und hat entsprechend zusammen mit dem Advisory eine aktualisierte Version der Software zum Download bereitgestellt. Als Workaround kann auf alternative Lösungen zurückgegriffen werden.

#### Expertenmeinung:

Die beiden durch Secunia gefundenen Schwachstellen sind brisant, denn so lassen sich diese a) durch externe Angreifer initiieren sowie b) konstruktive Attacken umsetzen. Da der Kern von WinRAR auch bei vielen Antiviren-Lösungen zum Tragen kommt, wird es nur eine Frage der Zeit sein, bis Exploits die Runde machen werden. Es liegt nun an den Antiviren-Herstellern, so schnell wie möglich zu reagieren, um flächendeckende Attacken zu vermeiden.

### 3.23 Sun Java System Directory Server bis 5.2 HTTP Admin-Interface erweiterte Rechte

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 07.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1783>

Der Sun Java System Directory Server (früher Sun ONE Directory Server) stellt ein zentrales Verzeichnis für die Erfassung und Verwaltung von Identitätsprofilen, Zugriffsrechten sowie Informationen zu Anwendungs- und Netzwerkressourcen bereit. Wie Sun Microsystems meldet, existiert ein nicht näher beschriebener Fehler im HTTP Admin-Interface des Sun Java System Directory Server bis 5.2. Durch die Schwachstelle könne ein System komplett kompromittiert werden. Es sind keine Details oder ein Exploit zur Schwachstelle bekannt. Sun hat einen Patch herausgegeben.

#### Expertenmeinung:

Diese Schwachstelle ist sehr schwer einzuschätzen, weil nun wirklich praktisch keine Details bekannt sind. Es ist noch nicht mal publiziert worden, um was für einen Fehler es sich handelt. Dies könnte darauf schliessen lassen, dass das Problem sehr schwerwiegend ist und Sun daher das Risiko eines erfolgreichen Exploits und Angriffs so gering wie möglich

halten möchte. Entsprechend sollte man sich bemühen die Patches schnellstmöglich einzuspielen.

### 3.24 Mozilla Firefox bis 1.0.7 HTML iframe-Tag lange Attribute Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 05.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1782>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, wobei das aktuelle Ziel der Entwickler ein Marktanteil von 10 % darstellt. Tom Ferris entdeckte eine schwerwiegende Pufferüberlauf-Schwachstelle beim iframe-Tag. Dieser wird genutzt, um Inline-Frames darzustellen. Wird ein solcher mit überlangen Attributen umgesetzt, kann eine Denial of Service-Attacke initiiert werden. Zur gegenwärtigen Stunde ist nicht klar, ob sich darüber ebenfalls beliebiger Programmcode ausführen lässt. Zusammen mit dem Advisory wurde ein proof-of-concept Exploit publiziert. Als Workaround wird empfohlen, zwischenzeitlich nur vertrauenswürdige Seiten aufzusuchen oder auf ein alternatives Produkt zurückzugreifen.

#### Expertenmeinung:

Die Gegner von open-source Projekten werden es gerne sehen, dass auch ein populäres Browser-Projekt aus diesem Bereich die eine oder andere wirklich unschöne Schwachstelle aufweist. In der Tat muss man es den Entwicklern anlasten, beim Design wenigstens in diesem Belang die Sicherheit aus den Augen verloren zu haben. Hätte Mozilla ein höheres Mass an Popularität, wäre diese Schwachstelle weit bedeutender; vor allem für Gelegenheitsangreifer und Skript-Kiddies. Es bleibt zu hoffen, dass dieses Projekt in Zukunft von derlei Fehlern verschont bleiben wird.

### 3.25 Citrix MetaFrame Presentation Server 3.0 und 4.0 Richtlinie anderer Hostname umgehen

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 03.10.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1779>

Citrix MetaFrame ist eine kommerzielle Erweiterung zu Microsoft TerminalServer und erlaubt das Nutzen verschiedener Anwender einer Windows-Umgebung über das Netzwerk. Dieser Dienst ist mit dem seit Jahren unter Unix gebräuchlichen X11 vergleichbar. Mit dem Citrix MetaFrame Presentation Server können gewisse Restriktionen anhand von IP-Adressen, Server, Benutzer und Client-Namen gemacht werden. Gustavo Gurmandi entdeckte, dass ein lokale Manipulation der Konfigurations-Dateien das Filtern anhand des Client-Namens austricksen lässt. Dazu kann ganz einfach die Datei launch.ica mit dem Notepad editiert werden. Das Vorgehen ist unter anderem im Advisory der GrupoITPro Security Research Community dokumentiert. Citrix wurde frühzeitig über das Problem informiert.

#### Expertenmeinung:

Client-seitige Sicherungsmassnahmen sind immer ein gefährliches Spiel. Es ist nur eine Frage der Zeit, bis ein gewiefter Angreifer herausfindet, wie er die Gegebenheiten zu seinem Vorteil manipulieren kann. Wie auch bei Webapplikationen gilt in der Entwicklung von Netzwerksoftware: Sicherungsmassnahmen müssen immer serverseitig und vom Benutzer so abgeschottet wie möglich inszeniert werden.

### 3.26 RealNetworks RealPlayer bis 10.0.5.756 Fehlermeldung Format String

Einstufung: **kritisch**  
Remote: Ja  
Datum: 27.09.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1771>

Der Real Player der Firma Real Networks kann für das Abspielen der hauseigenen Real-Formate (RealAudio und RealVideo) genutzt werden. Die Software ist als Freeware-Version für Windows, Linux/Unix und Macintosh verfügbar. C0ntex entdeckte eine kritische Format String-Schwachstelle in RealNetworks RealPlayer sowie dem Helix Player bis 10.0.5.756 (Gold). Sehr detailliert, mit technischen Details und einem in C geschriebenen Exploit versehen wird im Advisory davon berichtet, dass ein Angreifer über Fehlermeldungen erweiterte Rechte erlangen könne. Wie unter anderem Secunia meldet, sei der Fehler bisher nur auf Unix-Systemen verifiziert worden. Andere Betriebssysteme könnten aber ebenso betroffen sein. Als Workaround wird empfohlen, entweder auf das Nutzen der Real-Produkte ganz zu verzichten

oder wenigstens nur Real-Dateien bekannter und vertrauenswürdiger Herkunft zu öffnen.

#### Expertenmeinung:

Diese Verwundbarkeit zeigt einmal mehr, dass harmlose Client-Applikationen für Angriffe missbraucht werden können. Vor allem das sofortige Veröffentlichen eines handlichen Exploits vermag diese Schwachstelle zu einem Renner zu machen.

### 3.27 Mozilla Firefox bis 1.0.7 Fenster öffnen erweiterte Rechte

Einstufung: **kritisch**  
Remote: Ja  
Datum: 23.09.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1767>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz - In einigen Bereichen kann das freie Produkt gar langsam mit dem Marktführer Microsoft Internet Explorer (MS IEX) gleichziehen. Wie im Zusammenhang mit der Veröffentlichung der Version 1.0.7 des Firefox bekannt geworden ist, existierten bis anhin einige wirklich kritische Schwachstellen im Produkt. Eine davon schlägt sich in einer Design-Schwachstelle im Zusammenhang mit dem Öffnen neuer Fenster nieder. Ein Angreifer kann darüber unter gewissen Umständen Seiteninformationen verstecken und gar auf schon geschlossene Fenster referenzieren. Technische Details oder ein Exploit zur Schwachstelle sind bisher nicht bekannt. Das Problem wurde in der jüngsten Version 1.0.7 des Firefox behoben. Ein Upgrade wird aufgrund der Vielzahl der publizierten Probleme dringendst empfohlen.

#### Expertenmeinung:

Man merkt, dass die Popularität der Mozilla-Produkte immer mehr zunimmt, denn genauso nehmen auch die Meldungen gefundener Schwachstellen zu. Dies stützt einmal mehr die These, dass die Verbreitung einer Software das Interesse der Angreifer weckt und diese mit mehr Intensität nach möglichen Schwachstellen Ausschau halten. Eine Vielzahl an Sicherheitslücken prasselte bisher auf das Mozilla-Projekt nieder. Keine gute Werbung, in der Tat - Obschon Mozilla immerwieder als Alternative zum beschmutzten Microsoft Internet Explorer empfohlen wird, wird voraussichtlich über längere Zeit auch das Mozilla-Pendant seine weisse Weste nicht sauber halten können.

Es scheint, als müsse der sichere Webbrowser erst noch entwickelt werden, denn Mozilla bringt die gleichen (Kinder-)Krankheiten mit, wie auch schon viele vergleichbare Projekte zuvor. Die zwiespältige Sachlage wird hitzig diskutiert; so zum Beispiel im Heise-Forum.

### 3.28 Mozilla Firefox bis 1.0.7 XMLHttpRequest erweiterte Rechte

Einstufung: **kritisch**  
Remote: Ja  
Datum: 23.09.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1763>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz - In einigen Bereichen kann das freie Produkt gar langsam mit dem Marktführer Microsoft Internet Explorer (MS IEX) gleichziehen. Wie im Zusammenhang mit der Veröffentlichung der Version 1.0.7 des Firefox bekannt geworden ist, existierten bis anhin einige wirklich kritische Schwachstellen im Produkt. Eine davon schlägt sich in einem Designfehler im Zusammenhang mit XMLHttpRequest nieder. Durch einen manipulativen Eingriff kann ein Angreifer beliebige HTTP-Fragen erzwingen und so weitere Attacken einleiten (z.B. Mit localhost-Zugriffen oder auf Hopping-Attacken). Technische Details oder ein Exploit zur Schwachstelle sind bisher nicht bekannt. Das Problem wurde in der jüngsten Version 1.0.7 des Firefox behoben. Ein Upgrade wird aufgrund der Vielzahl der publizierten Probleme dringendst empfohlen.

#### Expertenmeinung:

Man merkt, dass die Popularität der Mozilla-Produkte immer mehr zunimmt, denn genauso nehmen auch die Meldungen gefundener Schwachstellen zu. Dies stützt einmal mehr die These, dass die Verbreitung einer Software das Interesse der Angreifer weckt und diese mit mehr Intensität nach möglichen Schwachstellen Ausschau halten. Eine Vielzahl an Sicherheitslücken prasselte bisher auf das Mozilla-Projekt nieder. Keine gute Werbung, in der Tat - Obschon Mozilla immerwieder als Alternative zum beschmutzten Microsoft Internet Explorer empfohlen wird, wird voraussichtlich über längere Zeit auch das Mozilla-Pendant seine weisse Weste nicht sauber halten können. Es scheint, als müsse der sichere Webbrowser erst noch entwickelt werden, denn Mozilla bringt die gleichen (Kinder-)Krankheiten mit, wie auch schon viele vergleichbare Projekte zuvor. Die

zwiespältige Sachlage wird hitzig diskutiert; so zum Beispiel im Heise-Forum.

### 3.29 Mozilla Firefox bis 1.0.7 Unicode zero-width non-joiner Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 23.09.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1762>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz - In einigen Bereichen kann das freie Produkt gar langsam mit dem Marktführer Microsoft Internet Explorer (MS IEX) gleichziehen. Wie im Zusammenhang mit der Veröffentlichung der Version 1.0.7 des Firefox bekannt geworden ist, existierten bis anhin einige wirklich kritische Schwachstellen im Produkt. Eine davon schlägt sich in einer Pufferüberlauf-Schwachstelle im Zusammenhang mit Unicode zero-width non-joiner nieder. Ein Angreifer kann so beliebigen Programmcode ausführen lassen oder eine Denial of Service-Attacke umsetzen. Technische Details oder ein Exploit zur Schwachstelle sind bisher nicht bekannt. Das Problem wurde in der jüngsten Version 1.0.7 des Firefox behoben. Ein Upgrade wird aufgrund der Vielzahl der publizierten Probleme dringendst empfohlen.

#### Expertenmeinung:

Man merkt, dass die Popularität der Mozilla-Produkte immer mehr zunimmt, denn genauso nehmen auch die Meldungen gefundener Schwachstellen zu. Dies stützt einmal mehr die These, dass die Verbreitung einer Software das Interesse der Angreifer weckt und diese mit mehr Intensität nach möglichen Schwachstellen Ausschau halten. Eine Vielzahl an Sicherheitslücken prasselte bisher auf das Mozilla-Projekt nieder. Keine gute Werbung, in der Tat - Obschon Mozilla immerwieder als Alternative zum beschmutzten Microsoft Internet Explorer empfohlen wird, wird voraussichtlich über längere Zeit auch das Mozilla-Pendant seine weisse Weste nicht sauber halten können. Es scheint, als müsse der sichere Webbrowser erst noch entwickelt werden, denn Mozilla bringt die gleichen (Kinder-)Krankheiten mit, wie auch schon viele vergleichbare Projekte zuvor. Die zwiespältige Sachlage wird hitzig diskutiert; so zum Beispiel im Heise-Forum.

### 3.30 Mozilla Firefox bis 1.0.7 korrupte XBM-Bilder Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 23.09.2005  
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=1761>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz - In einigen Bereichen kann das freie Produkt gar langsam mit dem Marktführer Microsoft Internet Explorer (MS IEX) gleichziehen. Wie im Zusammenhang mit der Veröffentlichung der Version 1.0.7 des Firefox bekannt geworden ist, existierten bis anhin einige wirklich kritische Schwachstellen im Produkt. Eine davon schlägt sich in einer Pufferüberlauf-Schwachstelle im Zusammenhang mit XBM-Bildern nieder. Ein Angreifer kann so beliebigen Programmcode ausführen lassen. Technische Details oder ein Exploit zur Schwachstelle sind bisher nicht bekannt. Das Problem wurde in der jüngsten Version 1.0.7 des Firefox behoben. Ein Upgrade wird aufgrund der Vielzahl der publizierten Probleme dringendst empfohlen.

#### Expertenmeinung:

Man merkt, dass die Popularität der Mozilla-Produkte immer mehr zunimmt, denn genauso nehmen auch die Meldungen gefundener Schwachstellen zu. Dies stützt einmal mehr die These, dass die Verbreitung einer Software das Interesse der Angreifer weckt und diese mit mehr Intensität nach möglichen Schwachstellen Ausschau halten. Eine Vielzahl an Sicherheitslücken prasselte bisher auf das Mozilla-Projekt nieder. Keine gute Werbung, in der Tat - Obschon Mozilla immerwieder als Alternative zum beschmutzten Microsoft Internet Explorer empfohlen wird, wird voraussichtlich über längere Zeit auch das Mozilla-Pendant seine weisse Weste nicht sauber halten können. Es scheint, als müsse der sichere Webbrowser erst noch entwickelt werden, denn Mozilla bringt die gleichen (Kinder-)Krankheiten mit, wie auch schon viele vergleichbare Projekte zuvor. Die zwiespältige Sachlage wird hitzig diskutiert; so zum Beispiel im Heise-Forum.

## 4. Statistiken Verletzbarkeiten

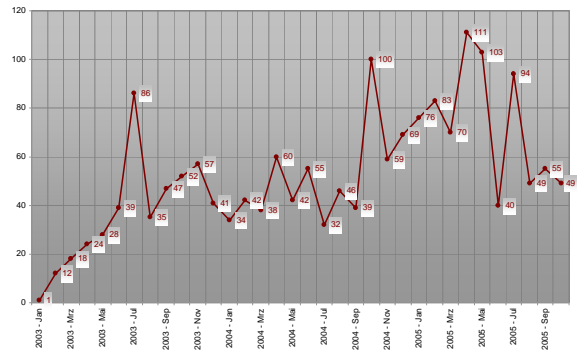
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



<http://www.scip.ch/cgi-bin/sms/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.

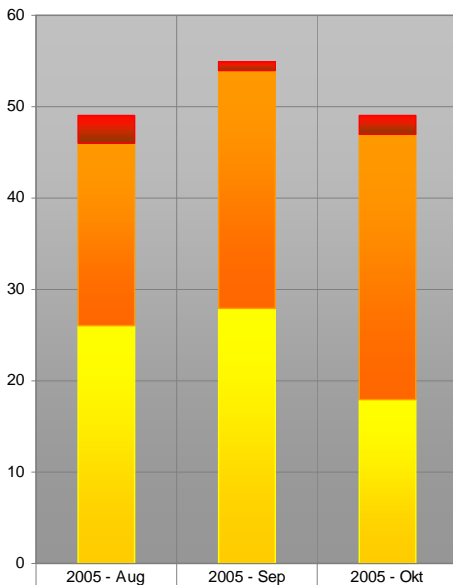
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat

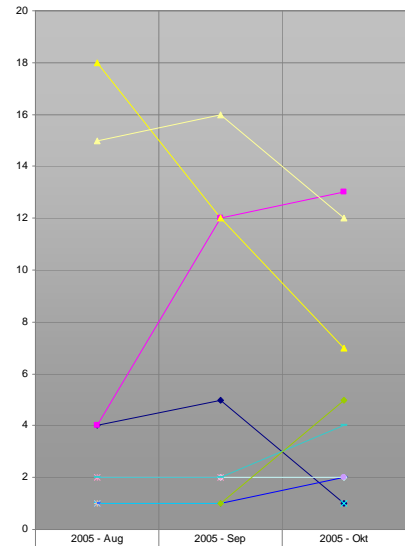
Auswertungsdatum:

19. Oktober 2005



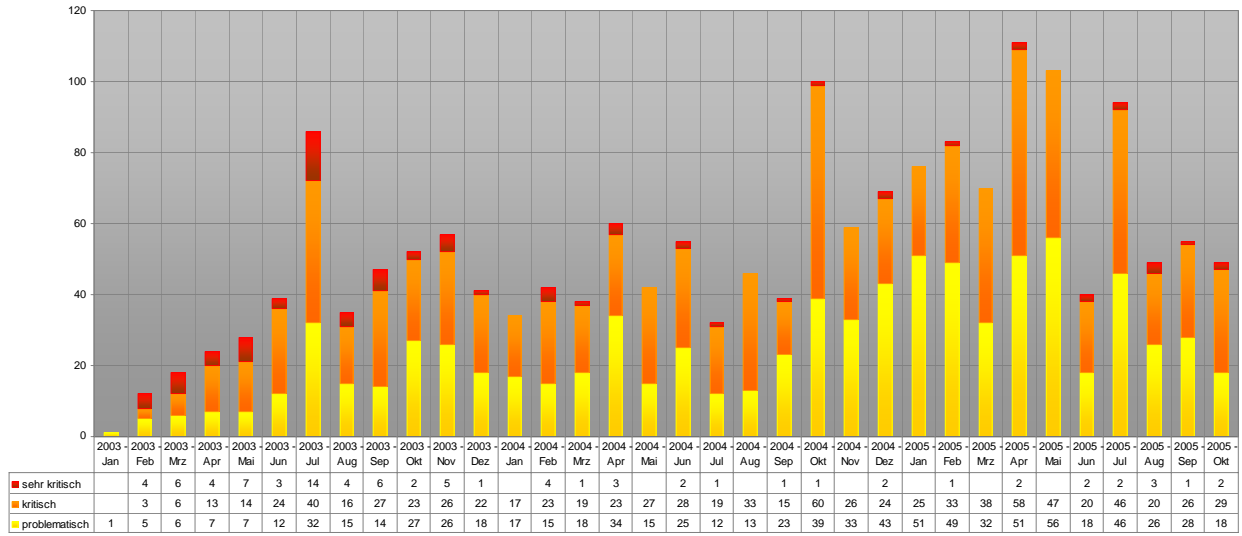
	2005 - Aug	2005 - Sep	2005 - Okt
sehr kritisch	3	1	2
kritisch	20	26	29
problematisch	26	28	18

Verlauf der letzten drei Monate Schwachstelle/Schweregrad

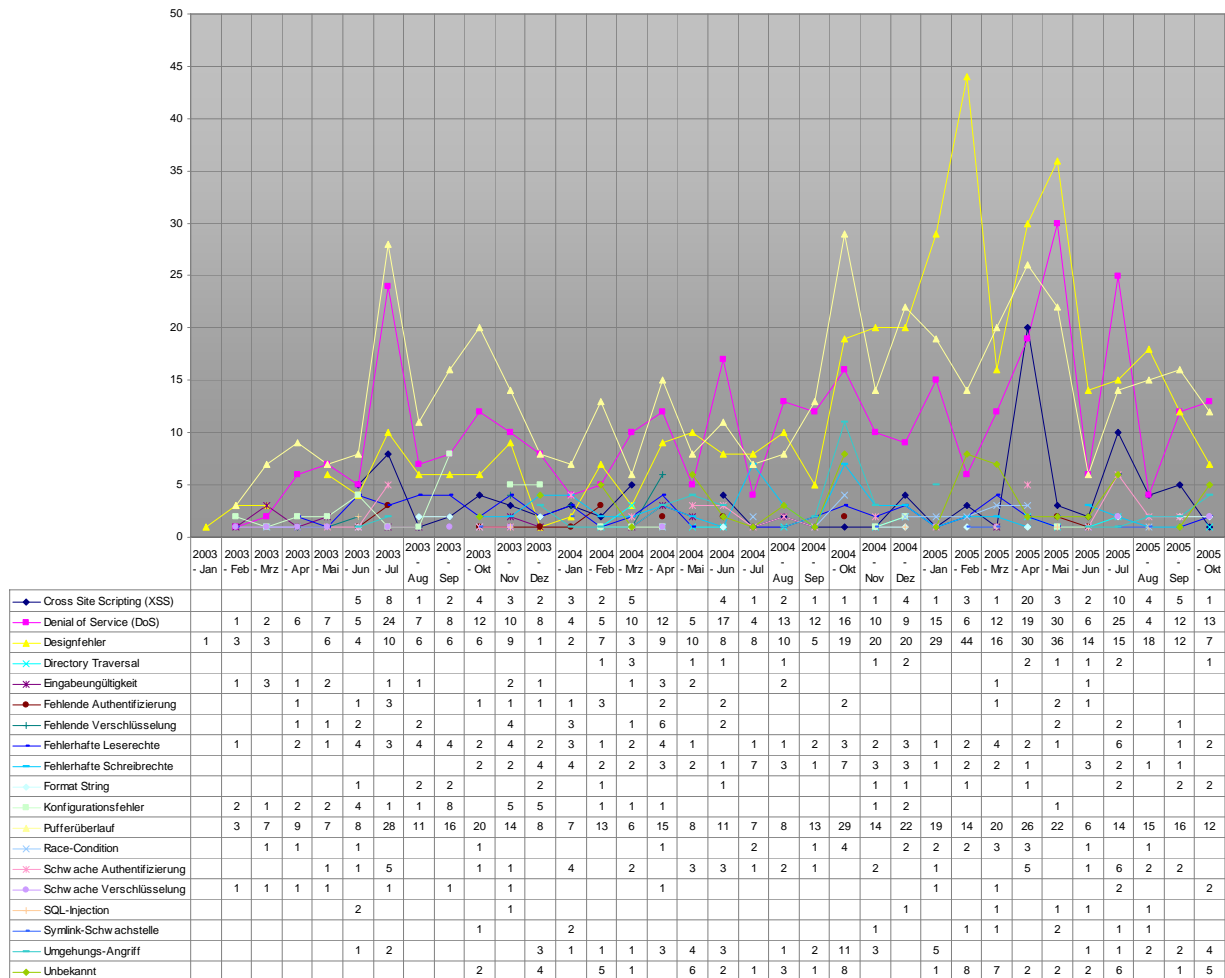


	2005 - Aug	2005 - Sep	2005 - Okt
Cross Site Scripting (XSS)	4	5	1
Denial of Service (DoS)	4	12	13
Designfehler	18	12	7
Directory Traversal			1
Eingabeungültigkeit			
Fehlende Authentifizierung			
Fehlende Verschlüsselung		1	
Fehlerhafte Leserechte		1	2
Fehlerhafte Schreibrechte	1	1	
Format String		2	2
Konfigurationsfehler			
Pufferüberlauf	15	16	12
Race-Condition	1		
Schwache Authentifizierung	2	2	
Schwache Verschlüsselung			2
SQL-Injection	1		
Symlink-Schwachstelle	1		
Umgehungs-Angriff	2	2	4
Unbekannt		1	5

Verlauf der letzten drei Monate Schwachstelle/Kategorie



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat



Verlauf der Anzahl Schwachstellen/Kategorie pro Monat

scip monthly Security Summary 19.10.2005





## 6. Literaturverzeichnis

scip AG, 2005, scip monthly Security Summary, Ausgabe April 2005

[http://www.scip.ch/publikationen/smss/scip\\_mss-19\\_04\\_2005-1.pdf](http://www.scip.ch/publikationen/smss/scip_mss-19_04_2005-1.pdf)

## 7. Impressum



Herausgeber:

scip AG

Technoparkstrasse 1

CH-8005 Zürich

T +41 44 445 1818

<mailto:info@scip.ch>

<http://www.scip.ch>



Zuständige Person:

Marc Ruef

Security Consultant

T +41 44 445 1812

<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 im Jahre 2002 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, 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](mailto:smss-feedback@scip.ch).

Das [Errata](#) (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online.

Der Bezug des scip monthly Security Summary ist **kostenlos**. [Anmelden!](#) [Abmelden!](#)