

## Contents

1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Kreuzworträtsel
5. Impressum

### 1. Editorial

#### Sicherheit erfordert Professionalität

Ich bin nun doch schon einige Jahre als Consultant für IT Security tätig. Habe schon so manches Problem gesehen, viele Projekte durchgemacht und immerwieder sonderbare Dinge erlebt. Wir alle kennen populäre Aussagen wie "Sicherheit ist ein Prozess". Dies, so heisst es an vielen Stellen immerwieder (z.B. Bruce Scheier), ist einer der Grundpfeiler der IT Security. Nein, keine Angst, ich wage es nicht, mich so weit aus dem Fenster zu lehnen und diese stets bewährte Postulation anzugreifen. Viel mehr möchte ich ihr einen entscheidenden Zusatz beifügen.

Meines Erachtens, und noch lange vor dem Prozess-Gedanken, kommt folgendes: "Sicherheit erfordert Professionalität".

Professionalität im herkömmlichen Sinne, wie man sie von einem Arzt erwartet. Sämtliche involvierten Personen wissen beispielsweise, worüber sie reden. Fehlt ihnen dieses Wissen oder besitzen sie nur "Halbwissen", dann haben sie dies offen zu kommunizieren und sich aus den jeweiligen Bereichen herauszuhalten.

Schon alleine dieser Grundsatz verhindert eine Vielzahl an Missverständnissen, Reibungen und

Unfällen in Bezug auf die Sicherheit. Wie oft kam es schon vor, dass in einer wichtigen Sitzung Dinge falsch koordiniert wurden, weil beispielsweise nicht alle Anwesenden die gleichen Begriffe nutzen oder unter ihnen nicht das gleiche verstehen?

Bestes Beispiel ist die immerwährende Differenz zwischen Security Audit, Penetration Test und Security Assessment. Ein deutscher Philosoph hat nicht umsonst in seiner Kritik festgehalten, dass dem Wort natürlicher Sprachen eine Vielzahl an historischen und individuellen Bedeutungen und Attributen beigemessen werden muss. Oder was verstehen Sie unter einem Security Audit? Und dieses Wort ist noch sehr jung!

Die Definition von zentralen Begriffen ist deshalb in wissenschaftlichen Arbeiten hoher Qualität stets ein Muss. Bestes Beispiel Erich Fromms Meisterwerk der Aggressionspsychologie, "Die Anatomie der Menschlichen Destruktivität" (1973), dessen erste Kapitel sich mit der Definition des Begriffs "Aggression" beschäftigen. Ohne diese Diskussion wäre das Buch voller Missverständnissen, wie man sie nur aus den Werken von Friedrich Nietzsche kennt.



Diese stoische Professionalität muss aber noch weitergehen, betrifft sie denn in erster Linie das Projektmanagement.

Weitsicht ist eine der Grundlagen dessen. Schon in der Offertphase gilt es eine kleine Roadmap mit den Milestones des Projekts sowie die möglichen

Probleme dieser festzuhalten. So kann spätestens beim Kickoff-Meeting mit dem Kunden auf die jeweiligen Gefahren hingewiesen werden, so dass sich das Risiko dieser minimieren lässt. Die grösste Gefahr für ein Projekt sind seine unkalkulierbaren da unvorhergesehenen Risiken.

Projektleiter und Verkäufer kommen nicht selten auf ihre technischen Mitarbeiter zu sprechen,

wenn es um das Abhandenkommen derlei Professionalität geht. Der Mut zur Wahrheit ("Nein, unser Produkt funktioniert noch nicht problemlos mit Betriebssystem X") und das Fehlen von wirtschaftlichem Fingerspitzengefühl wird ihnen ebenfalls negativ angelastet.

Doch umgekehrt sind die Vorwürfe in ihren Grundzügen nicht viel anders. Projektleiter und Verkäufer sind oftmals das direkte Bindeglied zum Kunden (jedenfalls denjenigen, die entscheiden und das Geld sprechen) - Verantwortung wird aber selten übernommen. Schon gar nicht in Situationen, in denen aufgrund des fehlenden technischen Fachwissens fehlerhafte Informationen weitergeleitet wurden. Der Druck von sich selbst wird dann genommen und auf die Techniker übertragen: Diese müssen halt die Leistung bringen, die der Kunde erwartet. In der Sozialpsychologie wird dies "kognitive Dissonanz" (nach Leon Festinger, 1957) genannt.

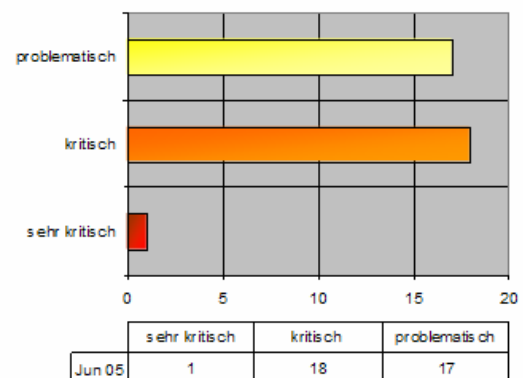
Der Mensch mit der Fähigkeit zu Denken und zu Kommunizieren sollte diese Interessenskonflikte überwinden können. Alle täten deshalb gut daran, zusammensitzten und die Differenzen und Ansichten zu diskutieren. Verkäufer würden verstehen, was sie überhaupt anzupreisen haben (und was nicht) - Und Techniker würden sehen, dass Geld in der Wirtschaft eine entscheidende Rolle spielt und dafür sorgt, dass sie was warmes zu Essen haben. Professionalität fängt also bei der Menschlichkeit an. Sie dort umzusetzen, das ist sicher am schwierigsten. Sicherheit erfordert Professionalität - Und Professionalität erfordert Menschlichkeit!

Marc Rued <maru-at-scip.ch>  
Security Consultant  
Zürich, 10. Juni 2005

## 2. scip AG Informationen

### 2.1 Verletzbarkeiten Monatsstatistik

Ab dieser Ausgabe des scip monthly Security Summary finden Sie die Statistik der in unserer Online Verletzbarkeitsdatenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> aufgenommenen Schwachstellen des entsprechenden Monats, zum Zeitpunkt der Publizierung des scip monthly Security Summary (smSS).



Die im smSS publizierten Schwachstellen sind nur ein Teil der jeweils in unserer Datenbank aufgenommenen Bugs. Die hier veröffentlichten Schwachstellen sollen nur einen Querschnitt darstellen.

### 3. Neue Sicherheitslücken

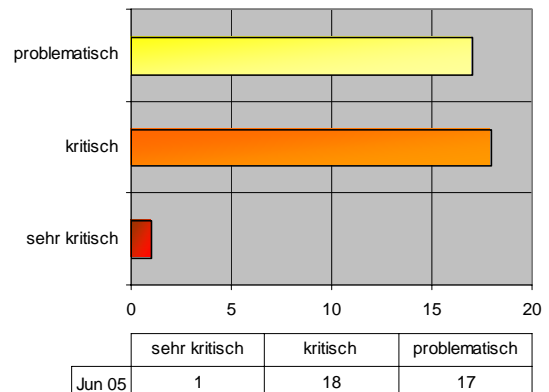
Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter <http://www.scip.ch/cgi-bin/smss/showadvf.pl> einsehbar.

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

#### Contents:

- 3.1 Adobe Acrobat/Reader 7.0.0 und 7.0.1 Local File Reading Vulnerability
- 3.2 Microsoft Outlook Express 5.5 und 6 News Reading Pufferüberlauf
- 3.3 Microsoft Exchange 5.5 Outlook Web Access Script Insertion Vulnerability
- 3.4 Microsoft Windows XP, 2000 und 2003 SMB Vulnerability
- 3.5 Microsoft Windows XP und 2003 Web Client Service Vulnerability
- 3.6 Microsoft Windows 2000, XP und 2003 HTML Help Input Validation Vulnerability
- 3.7 Microsoft Internet Explorer 5 und 6 PNG-Bilder Sicherheitsanfälligkeit
- 3.8 Sun J2SE 5.0 und J2SE 1.4.2\_07 für Windows, Solaris und Linux erweiterte Rechte
- 3.9 Sun Java Web Start (J2SE) 5.0 für Windows, Solaris und Linux Sandbox erweiterte Rechte
- 3.10 Macromedia verschiedene Produkte Licensing Service erweiterte Rechte
- 3.11 Apple MacOS X bis 10.4.1 AFP Server Pufferüberlauf
- 3.12 Sun Solaris 10 C-Bibliothek libc unbekannter Fehler
- 3.13 Mozilla Firefox bis 1.0.4 Cross Frame Injection
- 3.14 IBM WebSphere Application Server bis 5.0.2.11 Administrations-Konsole Authentisierung Pufferüberlauf
- 3.15 HP OpenView Application Manager mit Radia bis 4.x Notify Daemon Anfrage lange Dateierweiterung Pufferüberlauf
- 3.16 Microsoft Internet Explorer bis 6.0 JavaScript onload window() Denial of Service
- 3.17 Nortel VPN Router bis 5.05.200 IKE-Paket korrupter ISAKMP-Header Denial of Service
- 3.18 F5 BIG-IP bis 4.5.13, bis 4.6.3 und bis 9.1 TCP-Verbindungen Timestamp Denial of Service

- 3.19 Cisco Content Distribution Manager 4600 Series DNS-Paket Kompression Denial of Service
- 3.20 Cisco IP Phone 7902 korruptes DNS-Paket Kompression Denial of Service
- 3.21 BEA WebLogic bis 6.1 mit SP4 unbekannter Pufferüberlauf
- 3.22 BEA WebLogic bis 8.1 mit SP4 Eingabefelder Cross Site Scripting
- 3.23 CA eTrust Intrusion Detection Vet Antivirus Engine VetE.dll OLE-Stream Pufferüberlauf
- 3.24 CA eTrust Antivirus for the Gateway r7.0 und r7.1 Vet Antivirus Engine VetE.dll OLE-Stream Pufferüberlauf
- 3.25 Sun Solaris 9 und 10 in.ftpd ls mehrere \* Denial of Service



#### 3.1 Adobe Acrobat/Reader 7.0.0 und 7.0.1 Local File Reading Vulnerability

Einstufung: **problematisch**  
 Remote: Ja  
 Datum: 15.06.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1573>

Sverre H. Huseby hat eine Schwachstelle in Adobe Reader und Adobe Acrobat entdeckt. Durch das Ausnutzen der Schwachstelle, kann die externe Person an möglicherweise sensitive Informationen gelangen. Durch die Integration eines JavaScript in die PDF Datei, welches ein eingebundenes XML Dokument mit einer Referenz auf eine externe Quelle parst, kann es möglich sein, bestimmte Textdateien auf dem lokalen Computer zu lesen und an einen externen Standort zu senden. Betroffen sind 7.0.0 und 7.0.1. Ein Update auf 7.0.2 ist möglich oder als Workaround kann die Ausführung von

JavaScript innerhalb des Acrobat Reader deaktiviert werden.

#### Expertenmeinung:

Immer mehr Informationen werden in PDF-Dateien der breiten Öffentlichkeit zugänglich gemacht. Umso wichtiger ist es deren Inhalten vertrauen zu können. Ebenso unumgänglich ist das Vertrauen, beim Lesen eines PDF's keine ungewollten Aktionen aufzurufen, welche möglicherweise Dateien auf meinem Computer anderern sichtbar macht. Solche Verhaltensweisen kennen wir von Webbrowsern zur genüge... Hoffen wir, dass diese Art von Schwachstellen nicht die Runde macht und es keine Erweiterung dieser Zugriffe geben wird.

### 3.2 Microsoft Outlook Express 5.5 und 6 News Reading Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 14.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1572>

Danke NNTP können Meldungen abgerufen, verteilt und veröffentlicht werden, welche anschliessend den jeweiligen Bezüglern zur Verfügung stehen. Aufgrund einer nicht näher spezifizierten Buffer Overflow Schwachstelle in diesem Dienst, sieht sich ein Angreifer in der Lage die vollständige Kontrolle über ein betroffenes System erlangen. Somit wäre es ihm möglich Programme zu installieren, Daten Manipulation durchzuführen oder neue Konten mit sämtlichen Benutzerberechtigungen erstellen. Betroffen davon sind Microsoft Outlook Express 5.5 und 6.

#### Expertenmeinung:

Das im Betriebssystem Windows gratis enthaltene Outlook Express bot vor ca. 5 Jahren die Möglichkeit NNTP Meldungen via NNTP-Server zu beziehen. Der grosse Bruder MS Outlook bot diese Funktion nicht an. Zum Glück für Microsoft werden wohl die meisten Benutzer ihre News via RSS-Feed beziehen und nicht mehr via Network News Transfer Protocol (NNTP). Falls Sie dennoch NNTP benutzen und diese immer noch via Outlook Express lesen, sollten Sie den Patch schnellstmöglich applizieren.

### 3.3 Microsoft Exchange 5.5 Outlook Web Access Script Insertion Vulnerability

Einstufung: **kritisch**  
Remote: Ja  
Datum: 14.06.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1571>

Microsoft Outlook Web Access (OWA) wird durch den Exchange Server als Dienst bereitgestellt. Dank OWA kann ein Server, auf dem ein Exchange Server ausgeführt wird, auch als Website fungieren. Autorisierte Benutzer haben sodann, via Web, Zugriff auf Ihre E-Mails und ihren Kalender. Gaël Delalleau hat eine Schwachstelle rapportiert. Aufgrund dieser Scripting-Schwachstelle könnte es einem Angreifer ermöglichen, einen Benutzer zur Ausführung von gefährlichem Code zu verleiten. Das schädliche Skript wird dabei im Sicherheitskontext des Benutzers ausgeführt. Durch den Bug kann es einem Angreifer gelingen, auf beliebige Daten, die dem jeweiligen Benutzer zugänglich sind, auf dem Outlook Web Access-Server zuzugreifen..

#### Expertenmeinung:

Cross Site Scripting (XSS) Schwachstellen sind in diesem Jahr anscheinend der Renner. Immerhin benötigt es zur Ausnutzung dieser Schwachstelle eine Benutzeraktion. Doch nur zu gut wissen wir, dass dies bei geschickter Vorgehensweise nicht der Knackpunkt sein wird. OWA's sind immer speziell gefährdet, da ein Angreifer sich beim Zugriff auf dieses Systeme sensitive Daten erhofft. Auch hier gilt wieder, der geschulte und bewusste Benutzer minimiert das Risiko.

### 3.4 Microsoft Windows XP, 2000 und 2003 SMB Vulnerability

Einstufung: **kritisch**  
Remote: Ja  
Datum: 14.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1570>

Server Message Block (SMB) und Common Internet File System (CIFS), sind die Internetstandardprotokolle, die Windows zum gemeinsamen Verwenden von Dateien, Druckern und seriellen Anschlüssen sowie zur Kommunikation zwischen Computern verwendet. Dazu verwendet SMB Named Pipes und Mailslots. Durch eine nicht näher erläuterte Schwachstelle im SMB kann ein Angreifer von Extern beliebigen Codeausführen. Im schlimmsten Fall kann der Angreifer die vollständige Kontrolle über das betroffene System erlangen. Betroffen von dieser Schwachstelle sind Microsoft Windows 2000, XP und 2003.

#### Expertenmeinung:

Da technische Details fehlen, ist eine Einschätzung umso schwerer. Glücklicherweise sind, im Normalfall, Zugriffe auf SMB oder CIFS von externen Standorten respektive aus dem Internet nicht zugelassen. Unter Berücksichtigung der diesen Monat erschienen Schwachstellen und im Hinblick auf ein geschicktes Szenario, kann dieser SMB Bug dennoch von einem externen Angreifer ausgenutzt werden.

### 3.5 Microsoft Windows XP und 2003 Web Client Service Vulnerability

Einstufung: **kritisch**  
Remote: Ja  
Datum: 14.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1569>

Marck Lichtfield meldet eine Verletzbarkeit in Microsoft Windows. Dieser Bug erlaubt es einem lokalen Benutzer mit böser Absicht, unerlaubte Privilegien auf dem System zu erlangen und das ganze System zu kompromittieren. Dabei ein Angreifer Programme installieren, Daten anzeigen, ändern oder löschen oder neue Konten mit sämtlichen Benutzerberechtigungen erstellen. Um die Schwachstelle auszunutzen, muss man den Benutzer dazu verleiten auf den malicious WebDAV Service zu verbinden (zB via Webseite). Im Anschluss daran genügt es dem Web Client speziell präparierte Meldungen zu senden. Betroffen sind Microsoft Windows 2003 Server, XP Home Edition und Professional.

#### Expertenmeinung:

Der Patchday des Monats Juni hat es wirklich in sich. Erneut eine Schwachstelle, welche von extern ausgenutzt werden kann und Systemzugriff zulässt. Eine Hiobsbotschaft für alle Windows 2003 Verfechter. Immerhin stehen die Patches "Gewehr bei Fuss". Aus Erfahrung wissen wir dennoch, das zwischen der Bekanntgabe einer Schwachstelle und der Implementierung auf Seiten etwas grösserer Kunden, im Minimum zwei Wochen liegen. Betreiber aller Welt, macht Euch auf einen schönen Ende des Monats Juni gefasst.

### 3.6 Microsoft Windows 2000, XP und 2003 HTML Help Input Validation Vulnerability

Einstufung: **kritisch**  
Remote: Ja  
Datum: 14.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1567>

Windows Betriebssysteme sind aus unserem Alltag kaum noch wegzudenken. Viele Anwender schwören auf die Benutzerfreundlichkeit der Betriebssysteme der Firma von Bill Gates. Die HTML-Hilfe, zB via F1 Taste aufrufbar, ist zum wiederholtem Male ein Sicherheitsrisiko. Ein Angreifer sieht sich im Stande, durch das Ausnutzen der neusten Schwachstelle, die vollständige Kontrolle über das betroffene System zu erlangen. Da die meisten Benutzer mit "Admin"-Rechten auf ihren PC's arbeiten ist der Übernahme des Systemes Tür und Tor geöffnet. Betroffen sind Microsoft Windows 2000, 2000 Server, Server 2003, XP Home Edition und Professional. Die Patchentwickler von Microsoft haben sich die Freiheit genommen auch gleich ein, zwei weitere Sachen im zu patchenden System anzupassen. Dieser Umstand kann zu Problemen nach der Applizierung des Patches führen. Informationen dazu finden Sie im Link <http://support.microsoft.com/kb/896358>

#### Expertenmeinung:

Wiedereinmal beweist es sich als Bären dienst für Microsoft, dass die Benutzer mit Admin Rechten arbeiten. Respektive die Benutzer sind fast gezwungen mit "allen Rechten" zu arbeiten damit alles reibungslos funktioniert. Wer beschränkt sich schon gern selbst? Diese grundlegende Schwachstelle der Microsoft Betriebssysteme, welche ihnen zum Teil auch den Titel "broken by design" eingebracht haben, ist ein immer gern angegangenes Angriffsziel.

### 3.7 Microsoft Internet Explorer 5 und 6 PNG-Bilder Sicherheitsanfälligkeit

Einstufung: **sehr kritisch**  
Remote: Ja  
Datum: 14.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1565>

Der Microsoft Internet Explorer (MS IEX) ist fester Bestandteil moderner Windows-Betriebssysteme und damit der weitverbreiteste Webbrowser. Die Spezialisten der X-Force Gruppe haben eine Sicherheitsanfälligkeit bei der Verarbeitung zur Darstellung von PNG-Bildern gefunden. Durch das ausnutzen dieser Schwachstelle ist es einem Angreifer potentiell möglich, Code von extern, also remote, auf dem betroffenen System auszuführen. Nutzt ein Angreifer diese Sicherheitsanfälligkeit erfolgreich aus, kann er die vollständige Kontrolle über ein betroffenes System erlangen. Zur Ausnutzung dieser Schwachstelle genügt es die Person auf eine manipulierte HTML-Seite zu locken. Betroffen sind sowohl die Versionen des IEX 5 und IEX6 einschliesslich SP2. Die

Patchentwickler von Microsoft haben sich die Freiheit genommen auch gleich ein, zwei weitere Sachen im zu patchenden System anzupassen. Dieser Umstand kann zu Problemen nach der Applizierung des Patches führen. Informationen dazu finden Sie im Link 3.

#### Expertenmeinung:

Es scheint als ob sich Microsoft die schwerwiegenden Lücken auf den Juni aufgespart hat. Nach dem nicht erfolgten Patchday im Mai waren wir alle erstaunt. Die vorliegende Schwachstelle zeigt einmal mehr die Anfälligkeit der Webbrowser (bis jetzt nur IEX) auf. Bei jeder dieser beinahe zahllosen Schwachstellen weise ich immer wieder darauf hin, auf E-Mails im HTML Format zu verzichten. Egal wie schön diese gestaltet werden können, solange Sie Windows benutzen ist der IEX der Standardbrowser bei der Anzeige (die Mail-Previewansicht genügt, der Vorgang ist ja der selbe, der Code muss interpretiert werden...) dieser Mails. Ein solches manipuliertes Mail und Ihr System ist weder gepatcht noch mit weiteren Massnahmen geschützt, Pech gehabt. Da müssen Sie noch gar nicht auf einen Link drücken. Umsomehr verwundern mich die Marketingmails von Securityfirmen welche mich mit HTML-Mails zu Tagungen einladen. Glücklicherweise ist meine Policy so eingestellt, dass ich nur Plaintextmails empfangen kann, kein schöner Anblick - ein HTML in Plaintext...

### 3.8 Sun J2SE 5.0 und J2SE 1.4.2\_07 für Windows, Solaris und Linux erweiterte Rechte

Einstufung: **kritisch**

Remote: Ja

Datum: 13.06.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1564>

Java ist eine von Sun entwickelte plattformunabhängige Programmiersprache und nicht mit Java-Script zu vergleichen. Die Plattformunabhängigkeit wird dadurch erreicht, dass der kompilierte Programmcode zur Laufzeit interpretiert wird. Sehr gern wird Java auf Webseiten genutzt. Um den Missbrauch und erweiterte Rechte durch ein Java-Applet zu verhindern, wird dieses in einer sogenannten Sandbox ausgeführt. In dieser werden die Zugriffe auf Systemressourcen und Ressourcen anderer Benutzer oder Programme eingeschränkt oder gar verhindert. Aufgrund der vorliegenden Schwachstelle ist die korrekte Verarbeitung der gesetzten Regeln nicht mehr gegeben. Durch das ausnutzen dieser nicht

genauer spezifizierte Schwachstelle kann eine nicht vertrauenswürdige Applikation seine zugewiesenen Privilegien selbst erhöhen. Betroffen sind Java Web Start in Java 2 Platform Standard Edition (J2SE) 5.0 und 5.0 Update 1 für Windows, Solaris und Linux als auch and J2SE 1.4.2\_07 und Versionen vor 1.4.2 für Windows, Solaris und Linux.

#### Expertenmeinung:

Eine nicht näher spezifizierte Schwachstelle, welche es schwer macht diese selbst einzuschätzen. Dieses Problem zeigt einmal mehr auf, wie teilweise undurchdacht Java und seine Implementation sind. Der Skeptizismus gegenüber dieser plattformunabhängigen Sprache ist also auch weiterhin nachvollziehbar.

### 3.9 Sun Java Web Start (J2SE) 5.0 für Windows, Solaris und Linux Sandbox erweiterte Rechte

Einstufung: **kritisch**

Remote: Ja

Datum: 13.06.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1563>

Java ist eine von Sun entwickelte plattformunabhängige Programmiersprache und nicht mit Java-Script zu vergleichen. Die Plattformunabhängigkeit wird dadurch erreicht, dass der kompilierte Programmcode zur Laufzeit interpretiert wird. Sehr gern wird Java auf Webseiten genutzt. Um den Missbrauch und erweiterte Rechte durch ein Java-Applet zu verhindern, wird dieses in einer sogenannten Sandbox ausgeführt. In dieser werden die Zugriffe auf Systemressourcen und Ressourcen anderer Benutzer oder Programme eingeschränkt oder gar verhindert. Aufgrund der vorliegenden Schwachstelle ist die korrekte Verarbeitung der gesetzten Regeln nicht mehr gegeben. So kann eine nicht vertrauenswürdige Applikation seine zugewiesenen Privilegien selbst erhöhen. Als Beispiel kann die Applikation sich die Rechte zur Ausführung von Programmen auf welche der "ausgehebelte" Benutzer Zugriff hat oder ganz einfach Lese- und Schreibrechte vergeben. Betroffen sind Java Web Start in Java 2 Platform Standard Edition (J2SE) 5.0 und 5.0 Update 1 für Windows, Solaris und Linux. Java Web Start 1.0.1\_02 und frühere Version sind gemäss Aussagen des Herstellers nicht betroffen.

#### Expertenmeinung:

Eine nicht näher spezifizierte Schwachstelle, welche es schwer macht diese selbst

einzuschätzen. Glücklicherweise ist sowohl ein Patch als auch ein Workaround zur Beseitigung der Schwachstelle vorhanden. Somit können auch Firmen welche gerade Ihren "Patchrun" für diesen Monat durchhaben das Problem lösen. Dieses Problem zeigt einmal mehr auf, wie teilweise undurchdacht Java und seine Implementation sind. Der Skeptizismus gegenüber dieser plattformunabhängigen Sprache ist also auch weiterhin nachvollziehbar.

### 3.10 Macromedia verschiedene Produkte Licensing Service erweiterte Rechte

Einstufung: **kritisch**  
Remote: Indirekt  
Datum: 10.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1562>

Macromedia ist ein Hersteller verschiedener Produkte im Multimedia-Bereich. Wie der Hersteller meldet, existiert ein einer Reihe von Produkten (z.B. Macromedia Captivate, Macromedia Contribute 2 und 3, Macromedia Director MX 2004, Macromedia Dreamweaver MX 2004, Macromedia Fireworks MX 2004, Macromedia Flash MX 2004, Macromedia Flash MX Professional 2004, Macromedia FreeHand MX, u.a.) ein Designfehler in Bezug des Licensing Services. Ein Angreifer kann durch die Manipulation dessen erweiterte Rechte erlangen. Es sind keine Details oder ein Exploit zum Problem bekannt. Der Fehler wurde durch einen Hotfix für den Licensing Services behoben.

#### Expertenmeinung:

Da nahezu keine Details zur Schwachstelle bekannt sind, ist die Einschätzung sehr schwierig und zum jetzigen Zeitpunkt nur schwer möglich. Sollten Ihre Systeme verwundbar sein, sollen Sie schnellstmöglich auf eine aktuelle Software-Version updaten.

### 3.11 Apple MacOS X bis 10.4.1 AFP Server Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 09.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1549>

MacOS X ist ein relativ junges, kommerzielles, von der Firma Apple betreutes UNIX-Derivat. Es basiert auf OpenBSD und ist für Apple-Hardware verfügbar. Apple behebt mit dem Security Update 2005-006 einige kritische Sicherheitslücken in Apple MacOS X bis 10.4.1.

scip monthly Security Summary  
Marc Ruef & Simon Zumstein  
scip\_mss-19\_06\_2005-1.doc

Eine davon betrifft den AFP Server, der durch einen unbekanntem Pufferüberlauf beliebigen Programmcode ausführen liess. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Der von Apple herausgegebene Patch kann über das Internet bezogen werden.

#### Expertenmeinung:

Apple demonstriert sehr schön, wie schnell, kompetent und unkompliziert Schwachstellen in ihrem Betriebssystem behoben werden können. Das kumulative Security Update bringt die jeweiligen Systeme ohne grosse Umschweife wieder auf den neuesten Stand - Ein Zustand, der in der Microsoft-Welt nach wie vor nicht unbedingt zum Alltag gehört. Der Vorteil von Apple liegt sicher darin, dass sie auf ein als sicher geltendes, modular aufgebautes BSD gesetzt haben - In Punkto Sicherheit ein entscheidender Vorteil.

### 3.12 Sun Solaris 10 C-Bibliothek libc unbekannter Fehler

Einstufung: **kritisch**  
Remote: Ja  
Datum: 03.06.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1546>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. Der Hersteller hat im Alert 101740 einen unbekanntem Fehler in den C-Bibliotheken libc(3LIB) und libproject(3LIB) publiziert. Von der Schwachstelle betroffen ist einzig Sun Solaris 10. Der Fehler wurde mit den Patches 119689-02 für SPARC und 119689-03 für x86 behoben.

#### 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, 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.

### 3.13 Mozilla Firefox bis 1.0.4 Cross Frame Injection

Einstufung: **kritisch**  
Remote: Ja  
Datum: 06.06.2005  
scip DB: <http://www.scip.ch/cgi->

IT-Sicherheit Informationsammlung  
public

bin/smss/showadvf.pl?id=1543

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.. Brainsoft entdeckte einen rund 7 Jahre alten Fehler in Mozilla Firefox bis 1.0.4 [<http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=736>]. Das Hypertext Transfer Protocol (HTTP) ist die Grundlage des World Wide Webs (WWW). Der Client, im Normalfall ein Webbrowser wie der Internet Explorer, schickt eine HTTP-Anfrage an einen Server, der mit der Herausgabe der angeforderten Datei bzw. Daten reagiert. http-equiv meldete damals in einem kurzen Posting auf Full-Disclosure eine vermeintlich neue Sicherheitslücke im Microsoft Internet Explorer. Durch einen Fehler kann Fenster-übergreifend in andere Frames geschrieben und dort bösartige Dokumente geladen werden. Diese Cross Frame Injection ist nützlich für Social Engineering oder das Umgehen des Zonenmodells. Im Posting wurde auf <http://www.malware.com/targutted.html> verwiesen, das eine kleine Demo zusammen mit der WindowsUpdate-Webseite zeigt. Thomas Kessler wies darauf hin, dass es sich hierbei um ein altes Problem handelt, das für den Internet Explorer 3 und 4 mit Microsoft Security Bulletin (MS98-020; Patch Available for 'Frame Spoof' Vulnerability) behandelt wurde. Für diese Versionen stehen also Patches bereit. Die Versionen 5 bis 6 werden voraussichtlich bei einem Patch-Day mit entsprechenden Fixes folgen. Wie verschiedene Sicherheitsseiten meldeten, sind jedoch noch eine Reihe anderer Webbrowser von der Schwachstelle betroffen. Die Entwickler dieser stellten nach und nach Patches oder neue Versionen zur Verfügung. Das Mozilla Team hat noch nicht reagiert, wird aber voraussichtlich das Problem in einer zukünftigen Software-Version beheben.

#### Expertenmeinung:

Interessant ist an dieser Schwachstelle, dass sie eigentlich schon im Jahre 1998 bekannt war und auch behoben wurde. Der gleiche Fehler wurde aber scheinbar auch Jahre danach in den neuen Explorer-Versionen wieder gemacht oder übertragen. Dies zeugt nicht unbedingt von Verlässlichkeit der (Mozilla-)Entwickler. Ein solides Quality Management hätte dies verhindern sollen.

### 3.14 IBM WebSphere Application Server bis 5.0.2.11 Administrations-Konsole Authentisierung

### Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 03.06.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1542>

Die kommerzielle WebSphere Software von IBM ist eine universell einsatzfähige und schnelle Plattform für e-business on demand. Esteban Martínez Fayó entdeckte einen schwerwiegenden Pufferüberlauf in der Administrations-Konsole von IBM WebSphere Application Server bis 5.0.2.11. Dieser lässt sich bei der Authentisierung umsetzen und durch ihn beliebigen Programmcode ausführen. Zur erfolgreichen Ausnutzung des Fehlers muss die "global security option" aktiviert sein. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Der Fehler wurde im letzten Release der Software behoben.

#### Expertenmeinung:

Pufferüberlauf-Schwachstellen bei Passwort-Authentisierungen sind typische Klassiker. Sie erfreuen sich vor allem einem hohen Mass an Beliebtheit, weil jeder Remote-Anwender, der eine Verbindung zum Zielsystem herstellen kann, den Fehler für seine Zwecke ausnutzen könnte. Entsprechend geben die Entwickler von Authentifizierungs-Systemen sehr viel Acht darauf, dass ihre Mechanismen nicht so ohne weiteres überlistet werden können. Daher ist es sehr unangenehm für HP, einen solchen Fehler in ihrer Software einzugestehen.

### 3.15 HP OpenView Application Manager mit Radia bis 4.x Notify Daemon Anfrage lange Dateierweiterung Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 02.06.2005

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1541>

HP OpenView ist ein vor allem im professionellen Umfeld gern genutztes Produkt zur Überwachung von Systemen über das Netzwerk. Der Notify Daemon von Radia bis 4.x ist in Bezug auf lange Dateierweiterungen gegen eine Pufferüberlauf-Attacke verwundbar. So ist es über eine Anfrage möglich, beliebigen Programmcode ausführen zu lassen. Es sind keine genauen technischen Details oder ein Exploit zur Schwachstelle bekannt. HP hat einen Patch zum Problem herausgegeben.

**Expertenmeinung:**

Gleich zwei Pufferüberlauf-Schwachstellen, die zeitgleich im Notify Daemon von HP OpenView Application Manager mit Radia bis 4.x publiziert wurde. Es bleibt zu hoffen, dass nach diesem Fund eine genaue Inspizierung des Programmcodes umgesetzt wurde, um weitere Fehler dieser Art zu entdecken. Pufferüberlauf-Schwachstellen sind nach wie vor die populärsten Fehler mit der Möglichkeit zur konstruktiven Ausnutzung.

### 3.16 Microsoft Internet Explorer bis 6.0 JavaScript onload window() Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 31.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1537>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Benjamin Tobias Franz entdeckte eine kleine Denial of Service-Schwachstelle im Microsoft Internet Explorer bis 6.0. Und zwar kann über ein simples JavaScript bei gewissen Initialisierungen der Browser eingefroren werden. Dies kann beispielsweise mit [body onload="window();"] umgesetzt werden, wie unter anderem auch Secunia berichten. Unter anderem wird auch darüber spekuliert, dass sich durch diesen Fehler eigenen Programmcode ausführen lässt. Weitere technische Details zur Schwachstelle sind jedoch noch nicht bekannt. Microsoft hat noch nicht mit einem Patch reagiert. Stattdessen wird empfohlen, auf Active Scripting bei unbekanntem oder zwielichtigen Seiten zu verzichten bzw. auf einen alternativen Webbrowser (z.B. Netscape 8) auszuweichen.

**Expertenmeinung:**

Eine weitere Schwachstelle, die die Benutzer des verbreiteten Internet Explorer betrifft. Grundsätzlich handelt es sich um einen ärgerlichen Designfehler, der sich jedoch mit einer sichereren - aber wohl vielerorts unbrauchbaren - Konfiguration beheben lässt. Sollte sich jedoch wirklich herausstellen, dass sich über diesen Bug Programmcode ausführen lässt, sehen wir uns mit einem neuen Höchstmass an Risiko konfrontiert.

### 3.17 Nortel VPN Router bis 5.05.200 IKE-Paket korrupter ISAKMP- Header Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 30.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1536>

Die Firma Nortel hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Eine bekannte und gern genutzte Lösung ist durch die VPN Router gegeben. Die Modelle 1010, 1050, 1100, 600, 1600, 1700, 2600, 2700, 4500, 4600 and 5000 sind in den Versionen bis 5.05.200 gegen eine Denial of Service-Attacke verwundbar. So können diese Devices mit einem IKE-Paket mit einem korruptem ISAKMP-Header zum Absturz gebracht und zum Neustart bewegt werden. Es sind keine technischen Details oder ein Exploit zur Schwachstelle bekannt. Nortel wurde frühzeitig über das Problem informiert und hat schon am 27. Mai 2005 einen Patch zum Download bereitgestellt.

**Expertenmeinung:**

Diese Schwachstelle ist sehr interessant, da Nortel VPN-Lösungen vor allem im professionellen Bereich anzutreffen sind. Skript-Kiddies werden mit Sicherheit in den kommenden Wochen die neuen Möglichkeiten mal ausprobieren wollen. Entsprechend sind Gegenmassnahmen schnellstmöglich anzustreben.

### 3.18 F5 BIG-IP bis 4.5.13, bis 4.6.3 und bis 9.1 TCP-Verbindungen Timestamp Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 27.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1535>

F5 Networks ist Hersteller verschiedener Lösungen für high-end Load Balancing und Switching (vorwiegend auf Layer 7). Das mitunter bekannteste Produkt ist BIG-IP, das eben diese Funktionalität für grössere Netzwerke zur Verfügung stellt. Wie der Hersteller in seinem nur für Kunden zugänglichen Advisory meldet, ist dieses gegen eine wirklich unschöne TCP/IP-Schwachstelle - die auch Cisco betroffen hat - verwundbar. Werden nämlich in TCP-Segmenten fehlerhafte Timestamp-Werte genutzt, kann dadurch eine TCP-Sitzung eingefroren werden.

Diese wird erst wieder benutzbar, wenn sie zurückgesetzt wurde. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. F5 hat Patches für die jeweiligen Versionsreihen zum Download bereitgestellt.

**Expertenmeinung:**

Schon wieder ein Fehler diesen Monat in einem F5 Networks Produkt. Spekulationen wird damit guter Nährboden gegeben: Wird das Produkt erst jetzt wirklich eingesetzt und dadurch auf Herz und Nieren geprüft? Oder ist das nur ein dummer Zufall, dass zwei Sicherheitsprobleme praktisch zur gleichen Zeit publik werden? Wie dem auch sei täte auch F5 Networks gut daran, sich auf ein solides Quality Management zu verlassen, denn in der Sicherheitsbranche werden Fehler nur selten verziehen.

### 3.19 Cisco Content Distribution Manager 4600 Series DNS-Paket Kompression Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 24.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1528>

Die Firma Cisco hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Domain Name Service (Port 53 UDP, Port 53 TCP für Zone-Transfer) dient der Umwandlung von numerischen IP-Adressen in Domainnamen und umgekehrt, und er wird in den RFC 1032, 1033, 1034 und 1101 erläutert. Wie Cisco im Advisory 64994 meldet, existiert eine Denial of Service in mehreren ihrer Produkte im Umgang mit DNS. Und zwar kann ein korruptes DNS-Paket die Kompression/Dekompression negativ beeinträchtigen. Es ist eine Reihe verschiedener Produkte betroffen. Siehe dazu <http://www.cisco.com/warp/public/707/cisco-sn-20050524-dns.shtml#software>. Technische Details sind im NISCC Vulnerability Advisory 589088/NISCC/DNS enthalten. Ein Exploit zur Schwachstelle ist noch nicht bekannt. Für diese hat Cisco jeweils einen Patch zum Download bereitgestellt.

**Expertenmeinung:**

Angriffe über DNS sind für netzwerkfähige Systeme stets ein Problem, denn dieser Dienst wird praktisch immer und überall gerne genutzt. Dass es Cisco-Geräte trifft, ist natürlich für viele Cracker und Skript-Kiddies eine angenehme Sache. Denn die Popularität dieser Produkte verspricht eine Vielzahl verwundbarer Systeme.

Ein Exploit zur automatischen Ausnutzung der Schwachstelle dürfte also durchaus in Bälde folgen.

### 3.20 Cisco IP Phone 7902 korruptes DNS-Paket Kompression Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 24.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1519>

Die Firma Cisco hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Domain Name Service (Port 53 UDP, Port 53 TCP für Zone-Transfer) dient der Umwandlung von numerischen IP-Adressen in Domainnamen und umgekehrt, und er wird in den RFC 1032, 1033, 1034 und 1101 erläutert. Wie Cisco im Advisory 64994 meldet, existiert eine Denial of Service in mehreren ihrer Produkte im Umgang mit DNS. Und zwar kann ein korruptes DNS-Paket die Kompression/Dekompression negativ beeinträchtigen. Es ist eine Reihe verschiedener Produkte betroffen. Siehe dazu <http://www.cisco.com/warp/public/707/cisco-sn-20050524-dns.shtml#software>. Technische Details sind im NISCC Vulnerability Advisory 589088/NISCC/DNS enthalten. Ein Exploit zur Schwachstelle ist noch nicht bekannt. Für diese hat Cisco jeweils einen Patch zum Download bereitgestellt.

**Expertenmeinung:**

Angriffe über DNS sind für netzwerkfähige Systeme stets ein Problem, denn dieser Dienst wird praktisch immer und überall gerne genutzt. Dass es Cisco-Geräte trifft, ist natürlich für viele Cracker und Skript-Kiddies eine angenehme Sache. Denn die Popularität dieser Produkte verspricht eine Vielzahl verwundbarer Systeme. Ein Exploit zur automatischen Ausnutzung der Schwachstelle dürfte also durchaus in Bälde folgen.

### 3.21 BEA WebLogic bis 6.1 mit SP4 unbekannter Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 24.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1518>

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 mehrere Schwachstellen wurden in WebLogic gefunden. Der Hersteller berichtet im Advisory BEA05-82.00 von einem Pufferüberlauf in einer alten BEA WebLogic Version. Es sind keine weiteren Details oder ein Exploit bekannt. Der Fehler wurde im Service Pack 4 für BEA WebLogic 8.1 behoben.

#### Expertenmeinung:

Wieder einmal eine Hand voller Sicherheitslücken, die BEA mit einem Schlag publik macht und mittels Patch behebt. Grundsätzlich gut für die Anwender. Aber irgendwie keine gute Bilanz, denn sind fünf Schwachstellen doch ein bisschen viel für ein derlei professionelles Produkt - Und diese Situation ist nicht das erste Mal gegeben. Es fragt sich nämlich wirklich, ob da in dieser Lösung nicht noch andere Sicherheitslücken schlummern, die dem einen oder anderen Cracker schon bekannt sind. Aber erst die Zukunft wird es zeigen können, ob da wirklich Damokles' Schwert über den WebLogic-Administratoren schwebt.

### 3.22 BEA WebLogic bis 8.1 mit SP4 Eingabefelder Cross Site Scripting

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 24.05.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1516>

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 mehrere Schwachstellen wurden in WebLogic gefunden. ACROS berichtet im Advisory BEA05-80.00 von Cross Site Scripting- und Script-Injection Möglichkeiten über die Web-Schnittstelle. Es sind keine weiteren Details oder ein Exploit bekannt. Der Fehler wurde im Service Pack 6 für BEA WebLogic 7.0 behoben.

#### Expertenmeinung:

Wieder einmal eine Hand voller Sicherheitslücken, die BEA mit einem Schlag publik macht und mittels Patch behebt. Grundsätzlich gut für die Anwender. Aber irgendwie keine gute Bilanz, denn sind fünf Schwachstellen doch ein bisschen viel für ein

derlei professionelles Produkt - Und diese Situation ist nicht das erste Mal gegeben. Es fragt sich nämlich wirklich, ob da in dieser Lösung nicht noch andere Sicherheitslücken schlummern, die dem einen oder anderen Cracker schon bekannt sind. Aber erst die Zukunft wird es zeigen können, ob da wirklich Damokles' Schwert über den WebLogic-Administratoren schwebt.

### 3.23 CA eTrust Intrusion Detection Vet Antivirus Engine VetE.dll OLE-Stream Pufferüberlauf

Einstufung: **kritisch**  
 Remote: Ja  
 Datum: 22.05.2005  
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1505>

Ein Antivirenprogramm (auch Virenschanner) ist eine Software, die ihr bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspüren, blockieren und gegebenenfalls beseitigen soll. Eine Reihe von derlei Produkten wird durch die amerikanische Firma CA (Computer Associates) entwickelt und vertrieben. Alex Wheeler fand heraus, dass unter anderem CA eTrust Intrusion Detection eine Pufferüberlauf-Schwachstelle bei der Verarbeitung von OLE-Streams aufweisen. Der Fehler wird beispielsweise durch ein Word-Dokument provoziert und ist in der Vet Antivirus Engine, spezifisch in der Bibliothek VetE.dll, gegeben. Ein Angreifer sieht sich dadurch in der Lage, die Software zum Absturz zu bringen oder gar beliebigen Programmcode auszuführen. Einige technische Details sind im PDF-Advisory enthalten

[<http://www.rem0te.com/public/images/vet.pdf>] - Ein Exploit ist aber bisher noch nicht bekannt. CA hat ein Update der Vet engine auf 11.9.1 empfohlen. Als Workaround kann zwischenzeitlich eine alternative Antiviren-Lösung eingesetzt werden.

#### Expertenmeinung:

Dies ist natürlich ein Supergau für die Antiviren-Produkte von CA. Ein Virus kann nun nämlich ganz einfach daherkommen, und sich dem System während des Scan-Vorgangs bemächtigen. Die Antiviren-Lösung hat also quasi eine Einfallstür für das System geschaffen, obschon sie eigentlich genau das Gegenteil - die Erhöhung der Sicherheit der Umgebung - hätte gewährleisten können. Es ist nur eine Frage der Zeit, bis ein Virus die Runde macht, der eben genau diese Pufferüberlauf-Möglichkeit nutzt, um den Host zu übernehmen.

### 3.24 CA eTrust Antivirus for the Gateway r7.0 und r7.1 Vet Antivirus Engine VetE.dll OLE-Stream Pufferüberlauf

Einstufung: **kritisch**  
Remote: Ja  
Datum: 22.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1503>

Ein Antivirenprogramm (auch Virenschanner) ist eine Software, die ihr bekannte Computerviren, Computerwürmer und Trojanische Pferde aufspüren, blockieren und gegebenenfalls beseitigen soll. Eine Reihe von derlei Produkten wird durch die amerikanische Firma CA (Computer Associates) entwickelt und vertrieben. Alex Wheeler fand heraus, dass unter anderem CA eTrust Antivirus for the Gateway r7.0 und r7.1 eine Pufferüberlauf-Schwachstelle bei der Verarbeitung von OLE-Streams aufweisen. Der Fehler wird beispielsweise durch ein Word-Dokument provoziert und ist in der Vet Antivirus Engine, spezifisch in der Bibliothek VetE.dll, gegeben. Ein Angreifer sieht sich dadurch in der Lage, die Software zum Absturz zu bringen oder gar beliebigen Programmcode auszuführen. Einige technische Details sind im PDF-Advisory enthalten

[<http://www.rem0te.com/public/images/vet.pdf>] - Ein Exploit ist aber bisher noch nicht bekannt. CA hat ein Update der Vet engine auf 11.9.1 empfohlen. Als Workaround kann zwischenzeitlich eine alternative Antiviren-Lösung eingesetzt werden.

#### Expertenmeinung:

Dies ist natürlich ein Supergau für die Antiviren-Produkte von CA. Ein Virus kann nun nämlich ganz einfach daherkommen, und sich dem System während des Scan-Vorgangs bemächtigen. Die Antiviren-Lösung hat also quasi eine Einfallstür für das System geschaffen, obschon sie eigentlich genau das Gegenteil - die Erhöhung der Sicherheit der Umgebung - hätte gewährleisten können. Es ist nur eine Frage der Zeit, bis ein Virus die Runde macht, der eben genau diese Pufferüberlauf-Möglichkeit nutzt, um den Host zu übernehmen.

### 3.25 Sun Solaris 9 und 10 in.ftpd ls mehrere \* Denial of Service

Einstufung: **kritisch**  
Remote: Ja  
Datum: 25.05.2005  
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=1499>

Solaris ist ein populäres UNIX-Derivat aus dem Hause Sun Microsystems. Als Standard-FTP-Server wird in der Regel in.ftpd genutzt. Dieser ist gegen eine Schwachstelle verwundbar, die vor drei Monaten auch schon in wu.ftpd entdeckt wurde. Durch die Eingabe des Kommandos "dir [\*x128].\*" kann der FTP-Server unansprechbar gemacht werden. Das besagte Kommando führt dazu, dass sich eine Funktion immerwieder aufruft. Als Workaround wird empfohlen auf einen anderen FTP-Daemon zu wechseln, andernfalls nur vertrauenswürdigen Benutzern Zugriff zu gewährend und auf anonymes FTP zu verzichten. Ein Patch wurde von Sun zum Download bereitgestellt.

#### Expertenmeinung:

FTP-Server werden auf vielen Solaris-Systemen angeboten. Deshalb wird diese Schwachstelle mit offenen Armen empfangen. Zwar handelt es sich nur um einen Denial of Service-Fehler, mit dem in erster Linie die Nerven von Administratoren und Anwendern strapaziert werden können. Trotzdem muss mit einer Vielzahl an Zugriffen durch Skript-Kiddies, die mal eben rasch Spass haben wollen, gerechnet werden.

## 4. Kreuzworträtsel

John the Ripper	↘	Unix: Verschieben einer Datei	↘	Internet Protocol	Gruppenfamilie gemeinsame Zielsetzung	↘	Datenbank-Abfragesprache	↘	Zeichensatz für japanische Tastaturen	↘	↘	Packetstorm-Wettbewerb zu DDoS gewonnen	↘	Zentraleinheit eines Computers
Systemüberprüfung ob SW erworben wurde	↻ 6	Unix: Erzeugen eines Verzeichnisses	↗		UNIX-Kommando äquivalent zu dir unter DOS		Kleiner Bruder von Sendmail				↻ 7			Vorschlag NIST für Standard Digitale Signaturen
↙				Klassischer UNIX-Texteditor			Vorgänger des World Wide Web	↗					Unix: Speicherplatz jedes Verzeichnisses	
Gerät zur Datenübertragung via Telefonleitungen	Schichtmodell zur Kommunikation		↻ 1	Abk.: Internet Explorer			Kommandozeilen-Webbrowser		Intrusion Detection-System	↻ 3			Luftfahrtindustrie TLD	E-Mail Standard
↙					Wagenrückklau		Kommentare auf Nachrichten in Newsgroup							
DOS-Befehl Ausgabe Verzeichnisinhalten				Linux: Kopiert Dateien						Pufferüberlauf behaltetes Sendmail-Kommando				So weit ich weiss
↙				Feature pack von Checkpoint			DOS: Löscht Dateien				Les- und Schreibbarer Speicher			
Meiner bescheidenen Meinung nach	Unix: Online Hilfe	Autor von "TCP/IP Netzwerke"	↘		Datenkontrollsprache (in SQL)	↘	↻ 4		Einer der ersten Backdoors in Sendmail		Hersteller von Netzwerkelementen	↻ 8		
↙				Übertragung multimedialer Inhalte auf Mobiles										
↙							Deutscher Hacker-Club							
Schnittpunkt der Dateneübertragung	↻ 9	↻ 2	Backdoor		Wer behauptete, Linux hätte Quelltext gestohlen									
Künstliche Intelligenz	Webserver von Microsoft				Verschlüsselungs-Mech. für HTTP	↘			Interne Programmiersprache bei MS Word					
↙				Vorgänger von Windows 2000	optische Platte		↻ 5							
↙														
TCP-Flagge höfliche Beenden einer Sitzung														

### Wettbewerb

Mailen Sie uns das erarbeitete Schlüsselwort 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 **15.07.2005**. 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 der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

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

**SECURITYTRACKER**



## 5. Impressum

Herausgeber:

scip AG

Technoparkstrasse 1

CH-8005 Zürich

T +41 1 445 1818

<mailto:info@scip.ch>

<http://www.scip.ch>

Zuständige Person:

Marc Ruef

Security Consultant

T +41 1 445 1812

<mailto:maru@scip.ch>

PGP:

[http://www.scip.ch/firma/facts/maru\\_scip\\_ch.asc](http://www.scip.ch/firma/facts/maru_scip_ch.asc)

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. 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.

### Nutzen Sie unsere Dienstleistungen!

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserung 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!](#)