

Contents

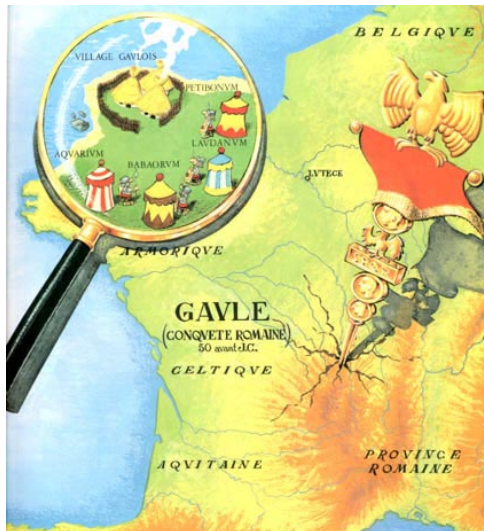
1. Editorial
2. scip AG Informationen
3. Neue Sicherheitslücken
4. Kreuzworträtsel
5. Literaturverzeichnis
6. Impressum

1. Editorial

Das Märchen vom Virus im Bild

Es war einmal vor langer Zeit ein junger Prinz, der sass sehr gerne vor seinem Computer. Vorwiegend schrieb er in BASIC kleine Programme, um seiner lieblichen Prinzessin zu imponieren. Irgendwann kam der weise Zauberer des Königshofs zu ihm und weihte ihn in die Geheimnisse der Computerviren ein. Ein neues Zeitalter brach an, in dem Feuer speiende Drachen längst nicht mehr die grösste Gefahr für Hof und Leute waren.

Der Prinz wusste nun, dass er keine Programme unbekannter oder zwielichtiger Herkunft öffnen durfte, da sich in ihnen ein Computervirus verbergen könnte. Als er das nächste Mal ein Email mit einem Bild als Anhang erhielt, rannte er sofort zum Zauberer und fragte, ob auch dieses die Gefahr eines Virus in sich barg. „Nein“, entgegnete der alte Mann energisch. „Viren sind Programmcode und können sich entsprechend nur in solchem weiterverbreiten. Habe keine Angst vor Bildern – Fürchte EXE-Dateien und dergleichen!“



Tja, das war vor langer Zeit so, denn in einer Welt, die mitunter von Cowboys aus Texas regiert wird, gilt dieser Grundsatz längst nicht mehr. Es stimmt, ein Virus muss ausgeführt werden können, damit er seiner Definition, der automatischen Vervielfältigung seiner selbst, gerecht wird. Doch Pufferüberlauf-Attacken und Skripting-Funktionalitäten machen es möglich, dass mittlerweile auch Programmcode über passive Dateiformate wie JPEG-Bilder und MP3-Musikdateien weiterverbreitet wird.

Jüngstes und imposantes Beispiel ist die den JPEG-Teil von Microsoft Windows betreffende Pufferüberlauf-Schwachstelle. Durch einen Programmierfehler ist es möglich, dass Windows beim Anzeigen eines korrupten Bildes beliebigen Programmcode ausführen lässt [scip 2004]. Angreifer können somit durch ein kleines JPEG-Bildchen neue Konten einrichten, Netzwerkverbindungen aufbauen oder einen Server starten. Schöne neue Welt, in der wir uns sogar vor Bildern fürchten müssen.

Was gilt es zu tun? Sind wir hilflos den Cowboys und Viren dieser Welt ausgeliefert? Nein! Ein kleines Dorf unbeugsamer Gallier leistet dem Eindringling erfolgreich Widerstand. Vorsicht ist nach wie vor und vor allem jetzt die Mutter der Porzellankeise. Emails unbekannter oder zwielichtiger Herkunft, egal ob aber vor allem mit Attachment, sollten unverzüglich gelöscht werden.

Die Hersteller von Software sind des weiteren angehalten, sich der immerwährenden Problematik von Sicherheitslücken durch fehlerhaftes Design oder unsaubere Softwareentwicklung vorzubeugen. Sicherheit muss in einer technokratischen Gesellschaft, wie wir sie nunmal hergezüchtet haben, gross geschrieben werden. Auch wenn dies manchmal auf Komfort und Wirtschaftlichkeit geht. Faulheit und Ignoranz werden nämlich über kurz oder lang dazu führen, dass das Internet ein für alle mal unbrauchbar wird. Dann kommen wir

3. Neue Sicherheitslücken

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

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

Contents:

- 3.1 Microsoft Internet Explorer bis 6 HTTP JavaScript execCommand() Dateiendung vortäuschen
- 3.2 Microsoft Internet Explorer bis 6 HTTP-Rückantwort Content-Location SP2 Sicherheits-Feature umgehen
- 3.3 Samba bis 3.0.7 QFILEPATHINFO spezieller Pfad Pufferüberlauf
- 3.4 Cisco Security Agent bis 4.0.3.728 mehrfacher Pufferüberlauf Umgehungs-Angriff
- 3.5 Cisco IOS 12.2(14)SZ und 12.2(18) DHCP korruptes Paket Flooding Denial of Service
- 3.6 Linux Kernel bis 2.4.27 und bis 2.6.8 ELF Binary Loader setuid erweiterte Rechte
- 3.7 Microsoft Internet Explorer bis 6.0 Macromedia Flash Link-Ziel vortäuschen
- 3.8 Mozilla Firefox bis 1.0 für Windows lokale Bilder DOS Gerätenamen Denial of Service
- 3.9 Microsoft Proxy Server 2.0 bis ISA Server 2000 DNS-Reverse-Lookup DNS-Cache Poisoning
- 3.10 RealVNC bis 4.0 TCP-Flooding 100 gleichzeitige Verbindungen Ports 5800 und 5900 Denial of Service
- 3.11 Microsoft Internet Explorer bis 6 URI res: Suchfenster existente Dateien erkennen
- 3.12 ISC DHCP bis 3.0b1-pl17 errwarn.c Logging Format String
- 3.13 Apache2 bis 2.0.52 HTTP-Anfrage mehrere Leerzeichen Denial of Service
- 3.14 Microsoft Internet Explorer HTML IFRAME SRC und NAME Pufferüberlauf
- 3.15 Perl bis 5.8.5 verschiedene Skripte erweiterte Rechte
- 3.16 libpng bis 1.0.17 png_read_png() Pufferüberlauf

3.1 Microsoft Internet Explorer bis 6 HTTP JavaScript execCommand() Dateiendung vortäuschen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 17.11.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=995>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. cyber flash publizierte zeitgleich zwei mittelschwere Schwachstellen im Microsoft Internet Explorer bis 6, die sich dazu nutzen lassen, um die neuen Sicherheits-Features des Service Pack 2 für Microsoft Windows XP zu umgehen. Eine davon betrifft die JavaScript-Funktion execCommand(), mit der Dateiendungen vorgetauscht werden können. Als Workaround wird empfohlen, den Download ausführbarer Dateien aus dem Internet zu verhindern (beispielsweise mittels Firewalling auf bekannte Dateierweiterungen). Zudem gilt es Active Scripting zu deaktivieren. Microsoft wird voraussichtlich mit einem Patch für das Problem reagieren.

Expertenmeinung:

Der Microsoft Internet Explorer ist einmal mehr unter heftigem Beschuss. Gleich mehrere nicht unkritische Schwachstellen haben den Weg in die Öffentlichkeit gefunden. Dies ist beste Werbung für den jüngst in der Version 1.0 erschienenen Webbrowser Mozilla Firefox. Der Internet Explorer ist somit zunehmend auf dem absteigenden Ast, was Microsoft sich selber zuzuschreiben hat.

3.2 Microsoft Internet Explorer bis 6 HTTP-Rückantwort Content-Location SP2 Sicherheits-Feature umgehen

Einstufung: **kritisch**
 Remote: Ja
 Datum: 17.11.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=994>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. cyber flash publizierte zeitgleich zwei mittelschwere Schwachstellen im Microsoft Internet Explorer bis 6, die sich dazu nutzen lassen, um die neuen Sicherheits-Features des Service Pack 2 für Microsoft Windows XP zu

umgehen. Wird in der HTTP-Rückantwort des Webservers ein bestimmter Wert in der Content-Location Zeile eingetragen, kann das neue Sicherheitsfeature zur Warnung beim Ausführen von heruntergeladenen Dateien nicht wahrnehmen. Als Workaround wird empfohlen, den Download ausführbarer Dateien aus dem Internet zu verhindern (beispielsweise mittels Firewalling auf bekannte Dateierweiterungen). Microsoft wird voraussichtlich mit einem Patch für das Problem reagieren.

Expertenmeinung:

Der Microsoft Internet Explorer ist einmal mehr unter heftigem Beschuss. Gleich mehrere nicht unkritische Schwachstellen haben den Weg in die Öffentlichkeit gefunden. Dies ist beste Werbung für den jüngst in der Version 1.0 erschienenen Webbrowser Mozilla Firefox. Der Internet Explorer ist somit zunehmend auf dem absteigenden Ast, was Microsoft sich selber zuschreiben hat.

3.3 Samba bis 3.0.7 QFILEPATHINFO spezieller Pfad Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 15.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=991>

Samba ist eine freiverfügbare Applikation für das Freigeben von Ressourcen (Datei- und Druckerfreigabe). Stefan Esser meldete dem Samba Team eine Pufferüberlauf-Schwachstelle in QFILEPATHINFO. Ist ein spezieller Pfad auf einer Samba-Freigabe vorhanden oder besitzt ein Angreifer Schreibrechte, kann er beliebigen Programmcode auf dem Zielsystem ausführen lassen. Genaue technische Details zur Schwachstelle oder ein Exploit sind nicht bekannt. Das Samba-Team hat die aktualisierte Version Samba 3.0.7 herausgegeben. Die jeweiligen Linux-Distributoren reagieren vorzu mit neuen Paketen. Zusätzlich wird empfohlen, nur vertrauenswürdigen Benutzern (Schreib-)Zugriff auf eine Samba-Ressource zu gewährend und grundsätzliche unerwünschte Zugriffe mittels Firewalling zu limitieren.

Expertenmeinung:

Problematisch ist diese Schwachstelle vor allem, weil der Samba-Daemon (smbd) meistens mit root-Berechtigung ausgeführt wird. Kann ein Angreifer die Schwachstelle ausnutzen, erbt er die Superuser-Privilegien. Grundsätzlich sollten keine Samba-Zugriffe aus unsicheren Netzwerken (z.B. dem Internet) zugelassen werden. Ein Firewall-System sollte die Datei- und

Druckerfreigabe lediglich in einem geschützten LAN erlauben. Aber trotzdem gilt es schnellstmöglich auf die aktuellste Samba-Version zu updaten, um mit dieser Sicherheitslücke den Angreifern nicht Tür und Tor zu öffnen – Zum Glück sind momentan noch keine Exploits zur automatisierten Ausnutzung der Schwachstelle publik.

3.4 Cisco Security Agent bis 4.0.3.728 mehrfacher Pufferüberlauf Umgehungs-Angriff

Einstufung: **kritisch**
Remote: Ja
Datum: 11.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=990>

Die ursprünglich von der amerikanischen Firma Okena entwickelte Software StormWatch ist eine echte Intrusion Prevention-Lösung. Durch Systemcall-Interception werden unerlaubte Kernel-Zugriffe abgefangen und unterbunden, so dass schwerwiegende Programmierfehler wie Pufferüberlauf-Schwachstellen nicht durch Angreifer ausgenutzt werden können [http://www.computec.ch/dokumente/intrusion_prevention/]. Vor einiger Zeit wurde diese Technik durch den Branchenriesen Cisco aufgekauft und neu unter dem Namen Cisco Security Agent (CSA) vertrieben. Wie nun bekannt wurde, existiert ein schwerwiegender Designfehler in Cisco Security Agent bis 4.0.3.728. Wird innerhalb von fünf Minuten ein Pufferüberlauf zum zweiten Mal umgesetzt, ist das IPS nicht in der Lage, den Angriff rechtzeitig abzufangen und zu unterbinden. Ein Angreifer kann so wie üblich seine Attacke erfolgreich umsetzen. Da der Agent selbst nicht bedroht ist, muss ein Angreifer eine Lücke im Betriebssystem oder einer Applikation finden, über die er Code einschleusen und ausführen kann. Erforderlich ist dazu jedoch, dass auf dem Zielsystem während der Angriffe ein Benutzer eingeloggt ist, da ansonsten der betroffene Software-Teil gekillt und neu gestartet wird. Als Lösung wird die Installation von Cisco Security Agent 4.0.3.728 oder neuer empfohlen. Als Workaround ist angeraten, die Lösung im Hidden User Interface Mode zu betreiben.

Expertenmeinung:

Okena StormWatch bzw. Cisco Security Agent ist im Verbund mit einer Antiviren-, Firewalling- und Intrusion Detection-Lösung am stärksten. Die einzelnen Elemente können in einem Gesamtkonzept die Schwächen der anderen ausbessern und so für ein Maximum an

möglicher Sicherheit in einer Umgebung sorgen. Genauso wie in diesem Fall hätte in den meisten Fällen ein automatisierter Wurm-Angriff in einem Netzwerk (z.B. W32.Blaster.Worm) trotz dem Fehler unterbunden werden.

3.5 Cisco IOS 12.2(14)SZ und 12.2(18) DHCP korruptes Paket Flooding Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 11.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=989>

Die Firma Cisco hat sich einen Namen mit ihren Netzwerkelementen - Switches und Router - gemacht. Internet Operating System (IOS) wird die Firmware von Cisco-Routern genannt. Der Hersteller meldet in seinem Document 63312 eine Denial of Service-Schwachstelle in Cisco IOS 12.2(14)SZ und 12.2(18). Wird eine entsprechende Cisco-Komponente als DHCP-Server oder Relay-Agent betrieben - was standardmässig der Fall ist -, kann durch den Versand mehrerer korrupter DHCP-Pakete die DHCP-Queue verstopft und dadurch eine Denial of Service provoziert werden. In der Folge verarbeitet der Router keine an ihn direkt gerichteten Pakete, etwa ARP und Routing-Protokolle, mehr. Auch der Managementzugriff über SSH oder SNMP ist dann nicht mehr möglich. Das Routing selbst funktioniert aber ganz normal weiter. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Cisco hat einen Patch für die betroffenen IOS-Versionen herausgegeben. Als Workaround wird empfohlen, entweder den DHCP-Dienst mittels "no service dhcp" zu deaktivieren oder im mindesten den bootps-Port mittels Firewalling bzw. ACL zu filtern.

Expertenmeinung:

Angriffe auf Cisco-Elemente sind aufgrund ihrer Verbreitung sehr beliebt. So kann man an dieser Stelle von Glück sprechen, dass sich dieser Remote-Angriff nur durchführen lässt, wenn auf dem verwundbaren System der DHCP-Dienst aktiviert ist. Wird dieses Feature nicht benötigt, sollte man es deaktivieren, um möglichst wenig Angriffsfläche zu bieten. Zusätzlich sollte man die neueste Version von IOS einspielen.

3.6 Linux Kernel bis 2.4.27 und bis 2.6.8 ELF Binary Loader setuid erweiterte Rechte

Einstufung: **kritisch**

Remote: Indirekt
Datum: 11.10.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=987>

Linux ist ein freies, UNIX-ähnliches Betriebssystem, das der General Public License (GPL) unterliegt. Es wurde 1991 vom Finnen Linus Torvalds ins Leben gerufen. Heute gilt es als grösster Konkurrent zum kommerziellen Windows-Betriebssystem aus dem Hause Microsoft. Ein Fehler im Linux-Kernel erlaubt es lokalen Angreifern, erweiterte Rechte zu erlangen. Das Problem liegt dabei im ELF Binary Loader, der teilweise im Umgang mit setuid-Dateien versagt. Technische Details sowie ein Exploit sind im Advisory von Paul Starzetz enthalten. Das Problem betrifft die Kernel bis 2.4.27 und bis 2.6.8 und wurden in den jüngsten Versionen behoben. Das Nutzen und Ausführen von setuid auf heiklen Partitionen sollte unterbunden werden. Zusätzlich wird empfohlen, nur vertrauenswürdigen Benutzern Zugriff auf Systeme zu gewähren.

Expertenmeinung:

Diese Sicherheitslücke ist sehr kritisch, wobei man jedoch von Glück sprechen kann, dass das Problem nur lokal ausnutzbar ist. Trotzdem sollte man sich schnellstmöglich bemühen, das eigene System entsprechend abzusichern. Vor allem Multiuser-Umgebungen dürften früher oder später durch diesen Fehler ein Problem kriegen.

3.7 Microsoft Internet Explorer bis 6.0 Macromedia Flash Link-Ziel vortäuschen

Einstufung: **kritisch**
Remote: Ja
Datum: 10.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=986>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Roozbeh Afrasiabi publizierte im Zusammenhang mit Macromedia Flash eine Schwachstelle im Microsoft Internet Explorer bis 6.0. So ist es durch eine Einbettung eines speziellen Flash-Elements möglich, die Destination eines normalen a href-Links vorzutäuschen. Diese Schwachstelle kann mitunter für die zur Zeit sehr populären Phishing-Angriffe genutzt werden. Von der Schwachstellen betroffen sind auf Microsoft Windows XP-Systeme mit installiertem Service Pack 2. Als Workaround wird das Deaktivieren der Funktion "Run ActiveX controls and plug-ins"

in den Einstellungen des Microsoft Internet Explorers oder das Nutzen eines alternativen Webbrowsers (z.B. Mozilla Firefox) empfohlen.

Expertenmeinung:

Die Welle an Designfehlern und anderweitigen Sicherheitsschwächen im Microsoft Internet Explorer reisst nicht ab und treibt die Benutzer zunehmend zu Alternativen wie Mozilla Firefox. Dies muss scheinbar eine wirklich ganz neue Sicherheitslücke sein, denn Microsoft hat sie noch nicht (klammheimlich) im letzten Service Pack 2 für Windows XP behoben.

3.8 Mozilla Firefox bis 1.0 für Windows lokale Bilder DOS Gerätenamen Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 10.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=983>

Das Mozilla-Projekt versucht einen open-source Webbrowser zur Verfügung zu stellen. Der Mozilla Webbrowser erlangte seit der Veröffentlichung der ersten offiziellen Versionen immer mehr Akzeptanz, kann jedoch in Punkto Marktanteile mit den anderen Grössen des Genres noch nicht mithalten. Zusammen mit der Veröffentlichung des ersten Major Releases 1.0 des Mozilla Firefox wurde eine Hand voll neuer Schwachstellen bekannt. So kann unter Umständen auf Windows durch das Referenzieren von DOS Device Names wie /dev/tty0 über lokale Bildern eine Denial of Service umgesetzt werden. Der Fehler wurde in der jüngsten Mozilla Firefox Version 1.0 behoben. Als alternative Lösung ist das Nutzen eines anderen Browsers (z.B. Opera oder Netscape) angeraten.

Expertenmeinung:

Wie schon in anderen Berichten und Einträgen in dieser Datenbank erwähnt, steigert die Popularität einer Software auch stets das Interesse der Angreifer am Finden von Schwachstellen in dieser. Der Trend ist bei Mozilla Firefox, der in den letzten Monaten immer bekannter wurde, sehr schön zu beobachten. Erstmals könnte man aber den jüngst bekannt gewordenen Schwachstellen schon fast vorwerfen, das sie der Bekanntheit des Firefox behilflich sind. Denn das Publizieren dieser Fehler fällt genau mit der Veröffentlichung der neuen Stable-Version 1.0 zusammen, die in den Medien gross angekündigt wurde. Wer also auch Nummer Sicher gehen will, der soll sich sowieso

die neue Fassung zu Gemüte führen.

3.9 Microsoft Proxy Server 2.0 bis ISA Server 2000 DNS-Reverse-Lookup DNS-Cache Poisoning

Einstufung: **kritisch**
Remote: Ja
Datum: 09.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=981>

Der Microsoft Internet Security and Acceleration Server (MS ISA, ehemals Microsoft Proxy Server) ist ein Application Gateway für Windows, das verschiedene Proxies zur Verfügung stellt. Martijn de Vries und Thomas de Klerk von Info Support International verhalfen zum Microsoft Security Bulletin MS04-039, in dem eine Designschwachstelle im Microsoft Proxy Server 2.0 bis ISA Server 2000 dokumentiert wird. Die Produkte speichern die Resultate eines DNS Reverse Lookups und nutzen diese bei einer normalen Namensauflösung. Ein Angreifer sieht sich somit in der Lage, DNS-Cache Poisoning zu betreiben und damit eigene Informationen in den DNS-Cache der Proxies einzuspeisen. Ein Spoofing von Webseiten ist somit möglich. SSL-Zertifikate sind davon natürlich nicht betroffen. Microsoft hat für die betroffenen Proxy-Versionen Patches zur Verfügung gestellt. Als Workaround wird empfohlen, den DNS-Cache zu deaktivieren.

Expertenmeinung:

Dies ist in der Tat ein schwerwiegender Fehler, der in keiner Firewalling-Lösung gegeben sein darf. Diese Schwachstelle zeigt natürlich sehr schön, dass die Proxy-Lösung noch immer mit Kinderkrankheiten zu kämpfen hat. Gerade da es sich um eine Sicherheitslösung handelt, ist diese Schwachstelle besonders ärgerlich. Um die Sicherheit in der eigenen Netzwerkumgebung gewährleisten zu können, sollte die verwundbare Funktion deaktiviert bzw. die Patches installiert werden.

3.10 RealVNC bis 4.0 TCP-Flooding 100 gleichzeitige Verbindungen Ports 5800 und 5900 Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 09.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=980>

VNC (Virtual Network Computing) überträgt per Netzwerk den gesamten Bildschirminhalt eines

Rechners auf einen andern und Mausclicks und Tastatureingaben in Gegenrichtung. RealVNC ist eine populäre Lösung des ursprünglichen VNC-Team von AT&T. Allan Zhang meldete, dass ein Server mittels TCP-Flooding mit rund 100 gleichzeitigen Verbindungen auf den Port 5900 zum Absturz gebracht werden kann. Dr_insane führt sodann weiter aus, dass auch der Port tcp/5800 von der Schwachstelle betroffen sei. Als Workaround wird empfohlen, den Zugriff auf die besagten Ports mittels Firewalling zu limitieren. Es ist damit zu rechnen, dass die Schwachstelle in einer zukünftigen Software-Version behoben werden.

Expertenmeinung:

Es ist schon ein bisschen erstaunlich, dass ein vermeintlich professionelles Entwickler-Team aus einer renommierten Firma wie AT&T einen grundsätzlichen Fehler bei der Netzwerkprogrammierung vorzuweisen hat. Flooding-Attacken sind zwar primitiv und nicht leicht abzufangen. Die hier vorgetragene Schwachstelle hingegen ist primär auf Unverständnis der Programmierer zurückzuführen.

3.11 Microsoft Internet Explorer bis 6 URI res: Suchfenster existente Dateien erkennen

Einstufung: **kritisch**
Remote: Ja
Datum: 09.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=977>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Benjamin Tobias Franz publizierte einmal mehr eine Sicherheitslücke in dem beliebten Browser. Microsoft Internet Explorer bis 6 kann die URI res: im Suchfenster genutzt werden, um die Existenz einer Datei auf dem lokalen System festzustellen. Dazu wird die Fehlermeldung "Access is Denied" abgewartet, die nur bei bestehenden Dateien auftritt. Ein proof-of-concept Exploit ist im Full-Disclosure Posting enthalten. Der Fehler wurde klammheimlich in Service Pack 2 für Microsoft Windows XP behoben. Es ist damit zu rechnen, dass in den kommenden Monaten ein dedizierter Patch für das Problem erscheinen wird.

Expertenmeinung:

Die Patch-Politik von Microsoft ist einmal mehr in höchstem Masse fragwürdig. So wurde das Problem insgeheim im Service Pack 2 für

Windows XP behoben. Kein Administrator oder Benutzer wusste bis dato von der bestehenden Sicherheitslücke. Microsoft denkt sich wohl, die Benutzer und Administratoren nicht unnötig mit Patches zu überhäufen. Aber dies ist mittel- und längerfristig definitiv der falsche Ansatz. Denn wer glaubt denn noch einem Hersteller, wenn dieser zu Gunsten der Einfachheit Probleme und Fehler verschweigt. Microsoft muss umdenken - Und zwar schnell!

3.12 ISC DHCP bis 3.0b1-pl17 errwarn.c Logging Format String

Einstufung: **kritisch**
Remote: Ja
Datum: 08.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=974>

DHCP (Dynamic Host Configuration Protocol) ist ein altbekanntes Protokoll zur dynamischen Verteilung von Netzwerkinformationen (z.B. IP-Adressen, Subnetzmasken, Default Gateways und Nameserver) an Hosts. Eine sehr bekannte und freie Implementierung dieses Dienstes wird von ISC, welche auch die Nameserver-Implementierung BIND entwickeln, zur Verfügung gestellt. Infamous41md meldet eine Format String-Schwachstelle in errwarn.c, die für das Logging verantwortlich ist. Ein Angreifer ist damit in der Lage, beliebigen Programmcode auf einem verwundbaren System auszuführen. Genaue Details zur Schwachstelle oder ein Exploit sind nicht bekannt. Von der Schwachstelle betroffen sind ISC DHCP bis 3.0b1-pl17. Als Lösung wird empfohlen, auf die aktuellste Software-Version upzugraden.

Expertenmeinung:

DHCP ist einer der Grundpfeiler moderner Netze. Gerade deshalb stellen Schwachstellen in den jeweiligen Implementierungen ein weitreichendes Risiko dar. In den meisten Fällen werden DHCP-Kommunikationen jedoch nur in lokalen Netzen bereitgestellt und erlaubt. Aber vor allem ISPs müssen mit einer Vielzahl potentieller Angreifer rechnen. Wer eine verwundbare DHCP-Version einsetzt, sollte deshalb umgehend diese aktualisieren oder anderweitig absichern.

3.13 Apache2 bis 2.0.52 HTTP-Anfrage mehrere Leerzeichen Denial of Service

Einstufung: **kritisch**
Remote: Ja
Datum: 02.11.2004
scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=964>

Apache ist ein populärer, freier open-source Webserver, der für viele verschiedene Plattformen erhältlich ist. Noam Rathaus von Beyond Security Ltd. Publiziert unter anderem auf SecuriTeam.com einen in Perl geschriebenen Exploit. Dieser setzt eine HTTP-Anfrage um, die mit einer Vielzahl an Leerzeichen beginnt, was zu einer Denial of Service führt. Von der Schwachstelle betroffen ist Apache2 bis 2.0.52. Die alten Versionen 1.x sind nicht verwundbar. Zur Zeit ist noch unklar, ob und inwiefern das Apache Team frühzeitig über die Schwachstelle informiert wurde. Es ist damit zu rechnen, dass dem Problem in einer kommenden Apache Version Rechnung getragen wird. In der Zwischenzeit wird empfohlen, entweder eine andere Webserver-Lösung einzusetzen oder betroffene Apache-Systeme mittels Firewalling zu schützen. Durch die direkte Integration vieler Linux-Distributionen von eigenen Apache-Ablegern, wird es in den kommenden Tagen zu etlichen dedizierten Patches der Linux-Distributoren kommen.

Expertenmeinung:

Der Angriff ansich ist primitiv - Genauso wie seine Auswirkungen. Genau dies wird ihn für Skript-Kiddies und dergleichen interessant machen. Dass eine relativ grosse HTTP-Anfrage zum Umsetzen der Denial of Service erforderlich ist, macht den Fehler aber hingegen wieder eher unpopulär. Trotzdem muss in den kommenden Tagen mit vermehrten Scans und DoS-Attacken auf Apache-Server gerechnet werden. Das Umsetzen von Gegenmassnahmen sollte deshalb nicht hinausgeschoben werden.

3.14 Microsoft Internet Explorer HTML IFRAME SRC und NAME Pufferüberlauf

Einstufung: **sehr kritisch**
 Remote: Ja
 Datum: 02.11.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=960>

Der Microsoft Internet Explorer (MS IEX) ist der am meisten verbreitete Webbrowser und fester Bestandteil moderner Windows-Betriebssysteme. Auf Full-Disclosure wurde von Berend-Jan Wever ein proof-of-concept Exploit publiziert, der eine Pufferüberlauf-Schwachstelle im HTML-Tag IFRAME ausnutzt [<http://www.securityfocus.com/archive/1/379261/>]. Dieser Tag wird angewendet, um in einem Webdokument eingebettete externe Frames zu laden. Der Pufferüberlauf betrifft die Attribute

SRC und NAME. Im Posting sind technische Details enthalten. Der mitgelieferte Exploit ist in reinem HTML geschrieben und öffnet eine Bindshell auf dem Port tcp/28876. Auf Full-Disclosure haben viele die Funktionsweise und Möglichkeiten des Exploits bestätigt. Der Empfang von HTML-E-mails und -Attachments per Email sollte mittels restriktiven Regeln auf dem SMTP-Relay bzw. Mailserver verhindert werden, um etwaige Wurm-Varianten und dergleichen zu unterbinden. Als Webbrowser sollte ein alternatives Produkt - zum Beispiel Mozilla Firefox - eingesetzt werden. Microsoft Windows XP mit installiertem Service Pack 2 ist nicht verwundbar. Es ist damit zu rechnen, dass Microsoft zum kommenden Patchday einen dedizierten Bugfix für den Internet Explorer zur Verfügung stellen wird.

Expertenmeinung:

Eine überaus sehr schwerwiegende Schwachstelle. Durch ein simples HTML-Dokument beliebigen Programmcode über einen Webbrowser auf einem System ausführen zu lassen, ist in der Zeit des World Wide Webs etwas vom schlimmsten. Der unverzüglich publizierte Exploit heizt das Ganze natürlich noch an, da er beweist, wie simpel und effizient sich der Fehler ausnutzen lässt. Für Microsoft heisst es nun, mit Hochdruck an einer spezifischen bzw. allgemeinen Lösung - nicht nur das SP2 für XP - zu arbeiten. In den kommenden Tagen muss mit einem extremen Aufkommen an Angriffen gerechnet werden.

3.15 Perl bis 5.8.5 verschiedene Skripte erweiterte Rechte

Einstufung: **kritisch**
 Remote: Indirekt
 Datum: 28.10.2004
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=955>

Perl ist eine offene und sehr populäre Skript-/Programmiersprache, die vor allem auf Linux-Systemen ihren Einsatz findet. Die speziell auf Sicherheit ausgerichtete Linux-Distribution Trustix weist auf eine Sicherheitslücke in Perl bis 5.8.5 hin, durch die lokale Benutzer erweiterte Rechte erlangen können. Mitunter sind Race Conditions und Symlink-Schwachstellen dafür verantwortlich. Genaue technische Details oder ein Exploit sind nicht bekannt. Die Sicherheitslücken wurden zum Grossteil in Perl 5.8.5 behoben. Als Workaround wird empfohlen, nur vertrauenswürdigen Benutzern lokalen Zugriff auf einem verwundbaren System zu gewähren oder eine andere Skripting- bzw. Programmiersprache für die Arbeiten zu nutzen.

Augenmerk stark auf derlei Angriffsflächen richten.

Expertenmeinung:

Lokale Schwachstellen sind für die meisten Angreifer uninteressant, da diese sich gar nicht erst zu den legitimen Benutzern zählen können. Auf Multiuser-Systemen ist das Risiko für die bestehenden Benutzer aber doch und durchaus gegeben. Vor allem dann, wenn die Vertrauenswürdigkeit der Anwender nicht zweifelsfrei festgestellt werden konnte (z.B. Bei Hosting-Angeboten oder Shell-Konten). In diesem Fall sollte dringendst über das Umsetzen von Gegenmassnahmen nachgedacht werden.

3.16 libpng bis 1.0.17 png_read_png() Pufferüberlauf

Einstufung: **kritisch**

Remote: Ja

Datum: 20.10.2004

scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=939>

libpng ist unter Unix und seinen Derivaten die Bibliothek für das darstellen des alternativen Grafikformats PNG. Der Linux-Distributor Debian meldet in ihrem DSA-570-1 eine Pufferüberlauf-Schwachstelle in libpng bis 1.0.17. Durch den Fehler in der Funktion png_read_png() kann ein Angreifer durch ein korruptes PNG-Bild die Library zum Abstürzen bringen oder gar beliebigen Programmcode ausführen lassen. Genaue technische Details oder ein Exploit zur Schwachstelle sind nicht bekannt. Die Sicherheitslücken wurden in libpng 1.0.17 behoben. Debian hat das Problem in 1.0.12-3.woody.9 sowie 1.0.15-8 für sid behoben. Andere Linux-Distributoren haben ebenfalls mit aktualisierten Paketen nachgezogen. Als Workaround wird empfohlen, auf das Nutzen bzw. Interpretieren von PNG-Dateien - vor allem aus unbekannter bzw. zwielichtiger Herkunft - zu verzichten. PNG-Bilder können zum Beispiel schon am Perimeter mittels Firewalling unterbunden werden.

Expertenmeinung:

Angriffe auf Grafikformate (und auch Soundformate) sind momentan stark im kommen. Sie beweisen zunehmend, dass selbst die Interpretation von scheinbar harmlosen Daten-Dateien zur Kompromittierung eines Systems führen können. So wie es scheint, haben die Entwickler in dieser Richtung zu wenig bewusst auf die Sicherheit geachtet, was ich jetzt nach und nach rächt. Den Stein wirklich ins Rollen gebracht hat schlussendlich die JPEG GDI+ Pufferüberlauf-Schwachstelle in Microsoft Windows. Die Angreifer-Gemeinde hat dadurch Blut geleckt und wird nun in Zukunft das

4. Kreuzworträtsel

Was veranstaltet der CCC nebst dem Congress			Wonach sucht Wellenreiter		Fernsehnorm	Netzname eines WLAN		Schach-Grossmeister		BackOffice			Taste für Sonderfunktionen	
Erste populäre Index-Suchmaschine								7						
					Forum of Incident Response and Security Teams					Computer Online Adventure		6		
Kleiner Bruder von Sendmail			Einheitliche Min. Datenbank	Grafische Zeichen und Gefühlsäusserung		Wagenrücklauf		Bedienoberfläche für OS/2		DOS: Benennt eine Datei um		Feature pack von Checkpoint		
UNIX-Kommando equivalent zu dir unter DOS	AES Auswahl Endspiel teilnehmer	Computer Emergency Response Team			1		American Registry for Internet Numbers			IDS von ISS				
		Objektorientierte Programmierung			Was wird mit Outlook empfangen	Machte mit Patent zu GIF von sich reden				Inkarnation eines Gottes (An/Hu)		Les- und Schreibbarer Speicher	Maskottchen der BSD-Systeme	
Anwälte, Steuerberater, Ärzte TLD	5					Asia Pacific Network Information Centre								
			Grafische Bedienoberfläche										2	
Top-Level-Domain von Schweden								Populärste deutsche Linux-Distribution	Zentraleinheit eines Computers					
		Prozedur aufruf auf entferntem Rechner												
Protokoll für das Übertragen von Daten								3						
		4	Verteiltes Dateisystem		Dateikon-trollblock		Protokoll für Adressumwandlungen							
Klassischer UNIX-Texteditor	Internet Protocol			Unix: Löschen einer Datei		Künstliche Intelligenz								
		optische Platte												

Wettbewerb

Mailen Sie uns das erarbeitete Schlüsselwort an die Adresse <mailto:info@scip.ch> inklusive Ihren Kontakt-Koordinaten. Das Los entscheidet über die Vergabe des Preises. Teilnahmeberechtigt sind alle ausser den Mitarbeiterinnen und Mitarbeitern der scip AG sowie deren Angehörige. Es wird keine Korrespondenz geführt. Der Rechtsweg ist ausgeschlossen.

Einsendeschluss ist der **15.01.2004**. Die GewinnerInnen werden nur auf ihren ausdrücklichen Wunsch publiziert. Die scip AG übernimmt keinerlei, wie auch immer geartete Haftung im Zusammenhang mit irgendeinem im Rahmen des Gewinnspiels an eine Person vergebenen Preises. Die Auflösung der Security-Kreuzworträtsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary und dann bei Errata.

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

SECURITYTRACKER



5. Literaturverzeichnis

scip AG (Marc Ruef), 14. September 2004,
Microsoft verschiedene Produkte JPEG GDI+
Parsing Pufferüberlauf, scip.ch,
<http://www.scip.ch/cgi-bin/smss/showadv.pl?id=833>

6. Impressum

Herausgeber:
scip AG
Technoparkstrasse 1
CH-8005 Zürich
T +41 1 445 1818
<mailto:info@scip.ch>
<http://www.scip.ch>

Zuständige Person:
Marc Ruef
Security Consultant
T +41 1 445 1812
<mailto:maru@scip.ch>
PGP:
http://www.scip.ch/firma/facts/maru_scip_ch.asc

Einem **konstruktiv-kritischen Feedback** gegenüber sind wir nicht abgeneigt. Denn nur durch angeregten Ideenaustausch sind Verbesserung möglich. Senden Sie Ihr Schreiben an smss-feedback@scip.ch.

Die ausgewiesenen IT-Security Spezialisten der scip AG verfügen, in diesem sehr komplexen sowie breitgefächerten Spezialgebiet, über jahrelang erarbeitetes und angewandtes Wissen. Wir sind der **effiziente** und **persönliche** Partner im Sektor IT-Sicherheit. Bei Fragen, Schulungen, Assessments und Projekten im Bezug zur IT-Security finden Sie eine kompetente Anlaufstelle in uns.

Nutzen Sie unsere Dienstleistungen!

Das Errata (Verbesserungen, Berichtigungen, Änderungen) der scip monthly Security Summary's finden Sie online unter <http://www.scip.ch/publikationen/smss/>.

Der Bezug des scip monthly Security Summary ist **kostenlos**. Sie können sich mit einer Email an die Adresse smss-subscribe@scip.ch eintragen. Um sich auszutragen, senden Sie Ihr Email an die Adresse smss-unsubscribe@scip.ch