scip ag

Contents

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

1. Editorial

Die Zukunft der angewandten IT-Sicherheit

Vor einiger Zeit ist jemand in meinem privaten Umfeld auf mich zugekommen und hat mich gefragt, wie sich wohl mein Berufsstand entwickeln wird. Ich habe darauf entgegnet, dass einerseits Sicherheitsberatungen im Allgemeinen und Sicherheitsüberprüfungen im Speziellen massgeblich von den generischen Entwicklungen im Computerbereich abhängig sind. Andererseits geht mit diesen eine soziologische, wirtschaftliche und juristische Entwicklung einher, die indirekten Einfluss ausüben wird.

Gerne möchte ich meine Prognosen für die kommenden Jahre vortragen. Dabei beschränke ich mich bewusst auf die angewandte IT-Sicherheit, der natürlich die theoretische IT-Sicherheit zugrunde liegt.

5 Jahre: Erneuerte Lehren und erweitertes Verständnis
Auch im Jahre 2010 trete ich immer wieder an Situationen heran, bei denen ich mir denke, dass man das vielleicht noch hätte 1995 durchgehen lassen können, der Sachverhalt heute aber nicht mehr tragbar und rechtfertigbar ist. Zum Beispiel dann, wenn in einem Finanzunternehmen eine forensische Untersuchung wegen Betrugs ansteht und sich die letzten Jahre niemand um die Etablierung, Aufrechterhaltung und Auswertung von Logs bemüht hat.

Ähnlich, jedoch nicht gleich, verhält es sich beim Umgang der Leute mit ihrer Privatsphäre. In der Epoche von Facebook, Twitter und Foursquare wird Exhibitionismus und Narzissmus gross geschrieben. Eigenschaften, die vor 10 Jahren noch als Manko angesehen wurden, werden heute gesellschaftlich toleriert, bisweilen gar erwünscht. Die kaufkräftige Generation der 14- bis 30-jährigen geht dabei sehr blauäugig mit ihren Daten um. Sind sie oftmals zu Jung, um sich an die Widerstände der 90er Jahre erinnern zu können, als sich der kritische Bürger in Bezug auf Volkszählungen und die Fichenaffäre empört hat. (Daran hat auch die Fichenaffäre 2.0 nichts geändert.)

Gerade die Generation Facebook wird wohl in absehbarer Zeit durch Datenpannen, Datendiebstahl und Datenverkäufe schmerzlich erfahren müssen, was ihre personenbezogenen Daten wert sind bzw. wie diese einem schaden können. Erste Anzeichen einer Kritik am laxen und fahrlässigen Umgang der Seitenbetreiber - allen voran Mark Zuckerberg von Facebook - sind in Blogs und Zeitungen zu vernehmen.

Als Folge davon wird der moderne Mensch bewusster mit seinen Daten umgehen, diese sensibler klassifizieren und deshalb nur noch einem ausgewählten Personenkreis zugänglich machen wollen. Die Abgabe der Kontrolle über Daten wird zunehmends verweigert werden wollen. Im selben Atemzug werden die Unternehmen unter diesem Druck bzw. vor diesem Bedürfnis teilweise nachgeben müssen. Datensicherheit und Informationssicherheit wird zu einem zentralen Bestandteil der gesellschaftlichen, wirtschaftlichen und juristischen Ordnung werden - Wenn auch vorerst nur in unliebsamer und zaghafter Weise.

15 Jahre: Weiterführende Automatisierung und Industrialisierung
Die angewandte Computersicherheit hat in den letzten 20 Jahren eine enorme Automatisierung und damit die Möglichkeit einer Industrialisierung erfahren. Dies ist sehr schön am Beispiel von Sicherheitsüberprüfungen zu illustrieren. Zu Beginn musste in mühsamer Weise mit manuellen Zugriffen eine Analyse umgesetzt werden. Werkzeuge wie Ping und Traceroute wurden eingesetzt, um einzelne Systeme zu testen.

© scip AG

Heutzutage können verschiedene Auswertungs- und Scanning-Utilities genutzt werden, die eine Sammlung der Grunddaten automatisieren oder wenigstens erleichtern. Eine einstündige Prüfung mit einem modernen Vulnerability Scanner hätte vor 15 Jahren noch mehrere Wochen gedauert. Durch die Automatisierung kann in der gesamten Computersicherheit die Wirtschaftlichkeit und Wissenschaftlichkeit erhöht werden.

Dieser Trend wird sich fortsetzen, obschon in den letzten Jahren eine gewisse Müdigkeit diesbezüglich festgestellt werden musste. Die Aufbruchsstimmung vor 10 Jahren konnte nicht anhalten, viele Projekte wurden kommerzialisiert und entwickeln sich deshalb langsamer oder konservativer. Zwar werden fortwährend neue Applikationen bereitgestellt, die die Umsetzung von Prüfungen professionalisieren helfen. Aufgrund des kommerziellen Hintergrunds dieser Lösungen sind sie jedoch nur für einen begrenzten Kreis von Benutzern interessant.

30 Jahre: Neue Konzepte und andere Herangehensweisen

Längerfristig wird sich der Bereich der Computersicherheit zu grossen Teilen verändern. Dies wird in erster Linie damit zu tun haben, dass Systemarchitekturen und Sicherheitskonzepte mit gänzlich anderen Herangehensweisen erstellt werden. Die Denkweise der Entwickler wird sich in grossen Teilen ändern und damit alte Angriffsmechanismen nicht mehr oder nur noch punktuell funktionieren.

So werden beispielsweise Eingabeüberprüfungen für "allgemeine" Anwendungen, wie zum Beispiel ein Webshop, sehr einfach und undiskutierbar implementierbar sein. Durch Module und Frameworks werden Vorlagen geliefert, mit denen Programmierer auch ohne grösseres Sicherheitsverständnis innert kürzester Zeit eine überdurchschnittliche Qualität erreichen können.

Geschlossene Systeme, können sich denn diese auch weiterhin breitflächig durchsetzen (siehe Apple mit iOS), helfen dabei, die Angriffsfläche für eine Vielzahl an technisch schwierig zu mitigierenden Schwachstellen zu eliminieren. Das Einschleusen von korruptem Programmcode, welches früher oder später im Rahmen eines umfassenden Angriffs erforderlich werden wird, wird damit massgeblich erschwert. Als wahrgenommene Restrisiken wird damit schlussendlich nur noch Social Engineering übrig bleiben, welches aufgrund des Faktor Mensch nie gänzlich eliminiert werden kann.

Als elementare Grundlage dieser neuen Ära wird der gänzlich andere Ansatz "Security First" dienen. Funktionalität wird nicht mehr pauschal und primär über Sicherheit gesetzt, da die Risiken einer Kompromittierbarkeit und die direkten Auswirkungen der Produktivität verstanden und akzeptiert werden. Dadurch können grundsolide Systeme konzipiert werden, die eine Anfälligkeit gegenüber "Patchwork-Lösungsansätzen" ausschliessen lassen können.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 6. September 2010

© scip AG

2. scip AG Informationen

2.1 Frohe Festtage

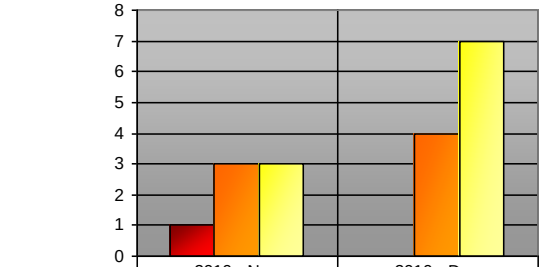
Die scip AG wünscht Ihnen frohe Festtage und einen guten und gesunden Rutsch ins neue Jahr 2010. Wir freuen uns darauf Sie auch im kommenden Jahr zu unserer Leserschaft begrüssen zu können.

© scip AG

3. Neue Sicherheitslücken

Die erweiterte Auflistung hier besprochener Schwachstellen sowie weitere Sicherheitslücken sind unentgeltlich in unserer Datenbank unter http://www.scip.ch/?vuldb einsehbar.

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



	2010 - Nov	2010 - Dez
sehr kritisch	1	0
kritisch	3	4
problematisch	3	7

Contents:

4232 NetBSD "udp6_output()" Denial of Service
4231 Microsoft Windows win32k.sys Driver "GreEnableEUDC()" Schwachstelle
4230 Microsoft Exchange Server RPC Denial of Service
4229 Microsoft SharePoint Document Conversions Launcher Service Schwachstelle
4228 Microsoft Windows Hyper-V VMBus Denial of Service
4227 Microsoft Windows Netlogon RPC Service Denial of Service
4226 Microsoft Windows OpenType Font Driver verschiedene Schwachstellen
4225 Microsoft Windows Routing and Remote Access NDProxy Pufferüberlauf
4224 Microsoft Windows Consent User Interface Privilege Escalation
4223 Mozilla Firefox verschiedene Schwachstellen
4222 Citrix Web Interface unspezifierte Cross Site Scripting Schwachstelle
4221 Winamp MIDI Timestamp Parsing Pufferüberlauf
4220 VMware Server verschiedene Schwachstellen

3.1 NetBSD "udp6_output()" Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 30.11.2010
scip DB: http://www.scip.ch/?vuldb.4232

NetBSD ist ein Unix-Derivat und gehört zur Familie der BSD-Betriebssysteme. Es wird unter der BSD-Lizenz frei vertrieben. Der Researcher Clement Lecigne beschreibt in einem Advisory eine Schwachstelle (Denial of Service (DoS)) in aktuellen Versionen der Applikation. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und - unter Umständen - beliebigen Code zur Ausführung bringen.

Expertenmeinung:
Diese Schwachstelle ist zwar nicht hochkritisch, kann aber je nach Umgebung und Art des Angriffs durchaus kritische Folgen haben. Betroffene Systeme sollten zeitnah mit Patches versorgt werden.

3.2 Microsoft Windows win32k.sys Driver "GreEnableEUDC()" Schwachstelle

Risiko: problematisch
Remote: Ja
Datum: 26.11.2010
scip DB: http://www.scip.ch/?vuldb.4231

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Ein Researcher mit dem Pseudonym "noobpwnftw" identifizierte unlängst eine Schwachstelle (Denial of Service (DoS)) in aktuellen Versionen der vorliegenden Applikation. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und damit den Betrieb des Systems und der entsprechenden Umsysteme empfindlich stören.

Expertenmeinung:
Während diese Schwachstelle nicht zwingend kritisch ist, sollte aufgrund des verbleibenden

© scip AG

Restrisikos das zeitnahe Einspielen entsprechender Patches angestrebt werden.

3.3 Microsoft Exchange Server RPC Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 14.12.2010
scip DB: http://www.scip.ch/?vuldb.4230

Der Exchange Server ist ein Groupware- und Nachrichtensystem der Firma Microsoft. Er findet vor allem in von Microsoft-Produkten geprägten Infrastrukturen Verwendung und eignet sich für alle Größen von Netzwerken. Es können beispielsweise Intranets aufgebaut und gepflegt, E-Mails verwaltet und gefiltert, Zeitpläne erstellt, Termine vereinbart und Diskussionen geführt werden. Die ZDI beschreibt in einem Advisory eine Schwachstelle (Denial of Service (DoS)) in aktuellen Versionen der Applikation. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:
Während diese Schwachstelle nicht zwingend kritisch ist, sollte aufgrund des verbleibenden Restrisikos das zeitnahe Einspielen entsprechender Patches angestrebt werden.

3.4 Microsoft SharePoint Document Conversions Launcher Service Schwachstelle

Risiko: problematisch
Remote: Ja
Datum: 14.12.2010
scip DB: http://www.scip.ch/?vuldb.4229

Microsoft Office SharePoint Server (kurz: MOSS) (zuvor bis Version 2003 SharePoint Portal Server, kurz: SPS) bezeichnet eine Portal-Software von Microsoft. Ziel des SharePoint Servers ist die Zusammenführung von Anwendungen und Datenquellen unter einer einheitlichen Weboberfläche. MOSS ist eine EAI- bzw. allgemeiner eine SOA-Plattform. Die ZDI veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Eingabeungültigkeit) in verschiedenen Versionen des Produktes beschreibt. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

Expertenmeinung:
Während diese Schwachstelle nicht zwingend kritisch ist, sollte aufgrund des verbleibenden Restrisikos das zeitnahe Einspielen entsprechender Patches angestrebt werden.

3.5 Microsoft Windows Hyper-V VMBus Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 14.12.2010
scip DB: http://www.scip.ch/?vuldb.4228

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Die Firma HP identifizierte unlängst eine Schwachstelle (Denial of Service (DoS)) in aktuellen Versionen der vorliegenden Applikation. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und - unter Umständen - beliebigen Code zur Ausführung bringen.

Expertenmeinung:
Diese Schwachstelle ist zwar nicht hochkritisch, kann aber je nach Umgebung und Art des Angriffs durchaus kritische Folgen haben. Betroffene Systeme sollten zeitnah mit Patches versorgt werden.

3.6 Microsoft Windows Netlogon RPC Service Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 14.12.2010
scip DB: http://www.scip.ch/?vuldb.4227

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Ein Duo von Researchern des Samba Teams beschreibt eine Reihe von Schwachstellen, vornehmlich der

© scip AG

Kategorie Denial of Service (DoS) in verschiedenen Versionen des Produktes. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und damit den Betrieb des Systems und der entsprechenden Umsysteme empfindlich stören.

Expertenmeinung:
Während diese Schwachstelle nicht zwingend kritisch ist, sollte aufgrund des verbleibenden Restrisikos das zeitnahe Einspielen entsprechender Patches angestrebt werden.

3.7 Microsoft Windows OpenType Font Driver verschiedene Schwachstellen

Risiko: kritisch
Remote: Ja
Datum: 14.12.2010
scip DB: http://www.scip.ch/?vuldb.4226

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Der Researcher Marc Schoenenfeld der Firma Red Hat Security Response Team veröffentlichte unlängst verschiedene Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

Expertenmeinung:
Die vorliegende Schwachstelle kann durchaus kritisch Auswirkungen nach sich ziehen. Betroffene Systeme sollten daher zeitnah gepatcht werden, um eine Kompromittierung zu vermeiden.

3.8 Microsoft Windows Routing and Remote Access NDProxy Pufferüberlauf

Risiko: problematisch
Remote: Ja
Datum: 14.12.2010
scip DB: http://www.scip.ch/?vuldb.4225

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Der Researcher Honggang Ren der Firma Fortinet beschreibt in einem Advisory eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der Applikation. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

Expertenmeinung:
Die vorliegende Schwachstelle kann durchaus kritisch Auswirkungen nach sich ziehen. Betroffene Systeme sollten daher zeitnah gepatcht werden, um eine Kompromittierung zu vermeiden.

3.9 Microsoft Windows Consent User Interface Privilege Escalation

Risiko: problematisch
Remote: Ja
Datum: 14.12.2010
scip DB: http://www.scip.ch/?vuldb.4224

Microsoft Windows ist ein Markenname für Betriebssysteme des Unternehmens Microsoft. Ursprünglich war Microsoft Windows eine grafische Erweiterung des Betriebssystems MS-DOS (wie beispielsweise auch GEM oder PC/GEOS). Inzwischen wurde dieser Entwicklungszweig zugunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Der Name Windows (engl.: Fenster) rührt daher, dass aktive Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Der Researcher Cesar Cerrudo der Firma Argeniss beschreibt in einem Advisory eine Schwachstelle (Designfehler) in aktuellen Versionen der Applikation. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

Expertenmeinung:
Diese Schwachstelle ist zwar nicht hochkritisch, kann aber je nach Umgebung und Art des Angriffs durchaus kritische Folgen haben. Betroffene Systeme sollten zeitnah mit Patches

© scip AG

versorgt werden.

3.10 Mozilla Firefox verschiedene Schwachstellen

Risiko: kritisch
Remote: Ja
Datum: 10.12.2010
scip DB: http://www.scip.ch/?vuldb.4223

Firefox ist ein freier Webbrowser des Mozilla-Projekts. Der seit Mitte 2002 entwickelte Open-Source-Webbrowser bietet die Möglichkeit, eine breite Palette an Erweiterungen zu implementieren. Firefox ist weltweit nach dem Internet Explorer der am zweithäufigsten genutzte Webbrowser. Im deutschen Sprachraum ist er seit Mitte 2009 mit aktuell 50,4 % (Stand: Ende September 2010) der meistgenutzte Browser vor dem Internet Explorer von Microsoft mit 36,8 %. Ein Kollektiv von Researchern veröffentlichte unlängst verschiedene Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Durch die Ausnutzung der vorliegenden Schwachstelle kann unter Umständen beliebiger Code zur Ausführung gebracht werden, was zur Kompromittierung des Systems führen kann.

Expertenmeinung:
Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah gepatcht werden.

3.11 Citrix Web Interface unspezifierte Cross Site Scripting Schwachstelle

Risiko: problematisch
Remote: Ja
Datum: 09.12.2010
scip DB: http://www.scip.ch/?vuldb.4222

Citrix Systems ist ein US-amerikanisches Softwareunternehmen, das 1989 von Ed Iacobucci gegründet wurde und jetzt in Fort Lauderdale in Florida ansässig ist. Citrix-Aktien werden an der NASDAQ unter dem Kürzel CTXS gehandelt. Citrix Systems ist in 35 Ländern aktiv. Bekannt geworden ist Citrix in erster Linie mit Applikations- und Terminalserver-Anwendungen. Das hat zur Folge, dass mittlerweile oftmals der Name der Firma "Citrix" als Synonym für eine solche Anwendung verwendet wird. In den letzten Jahren hat Citrix jedoch sein Produktportfolio durch eine Virtual Desktop Infrastructure Lösung (XenDesktop), SSL VPN-Lösungen (Access Gateway), Lösungen zur WAN-Optimierung (WANScaler), Lösungen zur Web-Applikationsbeschleunigung bzw. zu Web Application-Firewalls (NETScaler), Monitoring (Edge Sight) sowie Single Sign-on (Password Manager) und anderen Security-Lösungen erweitert. Die Firma Citrix beschreibt in einem Advisory eine Schwachstelle (Cross Site Scripting (XSS)) in aktuellen Versionen der Applikation. Die Schwachstelle erlaubt es dem Angreifer XSS (Cross Site Scripting) Angriffe durchzuführen und dadurch beliebigen Kontext im Browser des Opfers zur Ausführung zu bringen.

Expertenmeinung:
Da keine Details der Schwachstelle bekanntgegeben werden, ist eine konkrete Einstufung schwierig vorzunehmen. Es ist aber von einem mittleren bis hohen Risiko auszugehen.

3.12 Winamp MIDI Timestamp Parsing Pufferüberlauf

Risiko: kritisch
Remote: Ja
Datum: 07.12.2010
scip DB: http://www.scip.ch/?vuldb.4221

Winamp ist ein unter Windows verbreiteter Audio- und Medienspieler der Firma Nullsoft. Winamp ist in der Lage, MP1-, MP2-, MP3-, MP4-, (Ogg)Vorbis-, AAC-, MIDI-, MOD- (sowie viele Derivate), MPC- (per Plug-in), WAV-, WMA-, WMV- (seit Version 5.12 auch mit DRM), FLAC- sowie NSV-Dateien wiederzugeben, und unterstützt außerdem das Replaygain. Mit Eingabe-Plug-ins lässt sich die Liste der unterstützten Dateiformate beliebig erweitern. Winamp lässt sich außerdem durch Skins in seinem Aussehen dem eigenen Geschmack anpassen. Durch weitere Plug-ins kann man Winamp um zusätzliche Funktionen ergänzen, z. B. Erweiterungen der Benutzeroberfläche oder das Kodieren und Konvertieren in weitere Dateiformate. Der Researcher Peter Wilhelmsen der Firma Kryptos Logic identifizierte unlängst eine Schwachstelle (Pufferüberlauf) in aktuellen Versionen der vorliegenden Applikation. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

Expertenmeinung:
Die vorliegende Schwachstelle kann durchaus kritisch Auswirkungen nach sich ziehen. Betroffene Systeme sollten daher zeitnah gepatcht werden, um eine Kompromittierung zu vermeiden.

© scip AG

3.13 VMware Server verschiedene Schwachstellen

Risiko: kritisch
Remote: Ja
Datum: 03.12.2010
scip DB: http://www.scip.ch/?vuldb.4220

VMware, Inc., ist ein US-amerikanisches Unternehmen, das Software im Bereich der Virtualisierung entwickelt. Das Unternehmen wurde 1998 mit dem Ziel gegründet, eine Technik zu entwickeln, virtuelle Maschinen auf Standard-Computern zur Anwendung zu bringen. Das bekannteste Produkt ist VMware Workstation. Der Hersteller VMware beschreibt eine Reihe von Schwachstellen, vornehmlich der Kategorie Pufferüberlauf in verschiedenen Versionen des Produktes. Ein Angreifer kann durch die vorliegende Schwachstelle beliebigen Code zur Ausführung bringen und somit die Kompromittierung des Systems anstreben.

Expertenmeinung:
Die vorliegende Schwachstelle ist als kritisch zu betrachten und sollte zeitnah gepatcht werden.

© scip AG

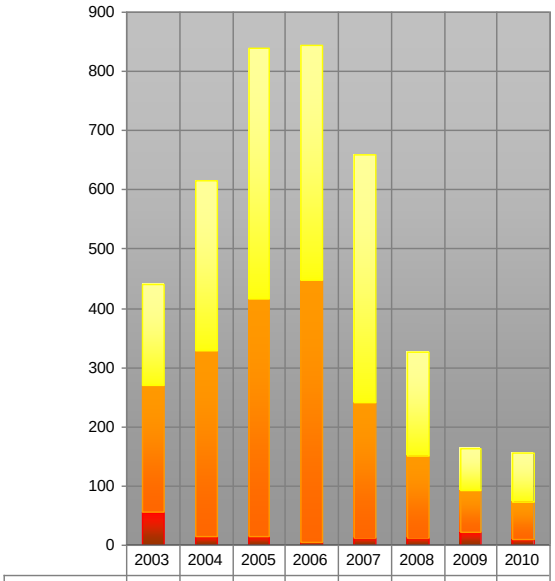
4. Statistiken Verletzbarkeiten

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

http://www.scip.ch/?vuldb

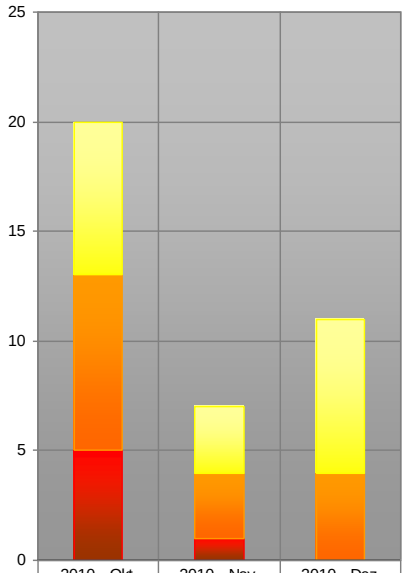
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an mailto:info@scip.ch. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum:	19. Dezember 2010



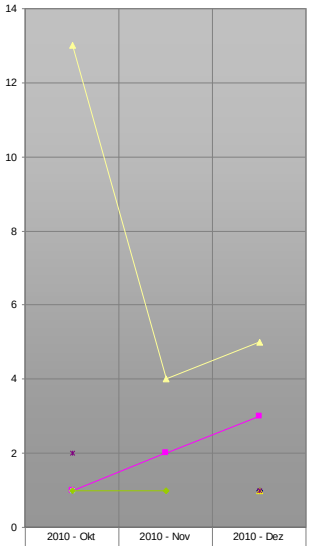
	2003	2004	2005	2006	2007	2008	2009	2010
problematisch	170	287	423	396	419	176	70	81
kritisch	214	314	402	442	229	140	72	64
sehr kritisch	56	15	15	6	11	11	21	10

Verlauf der Anzahl Schwachstellen pro Jahr



	2010 - Okt	2010 - Nov	2010 - Dez
problematisch	7	3	7
kritisch	8	3	4
sehr kritisch	5	1	

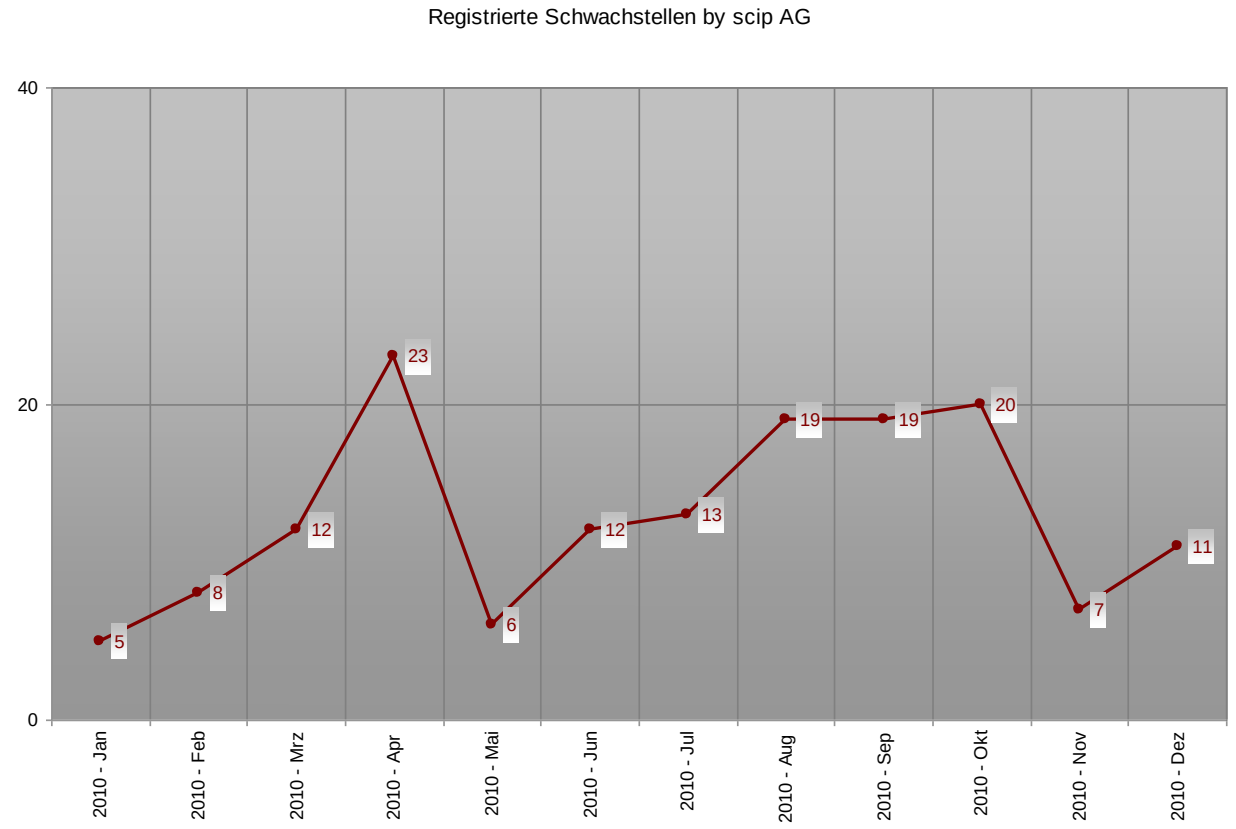
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



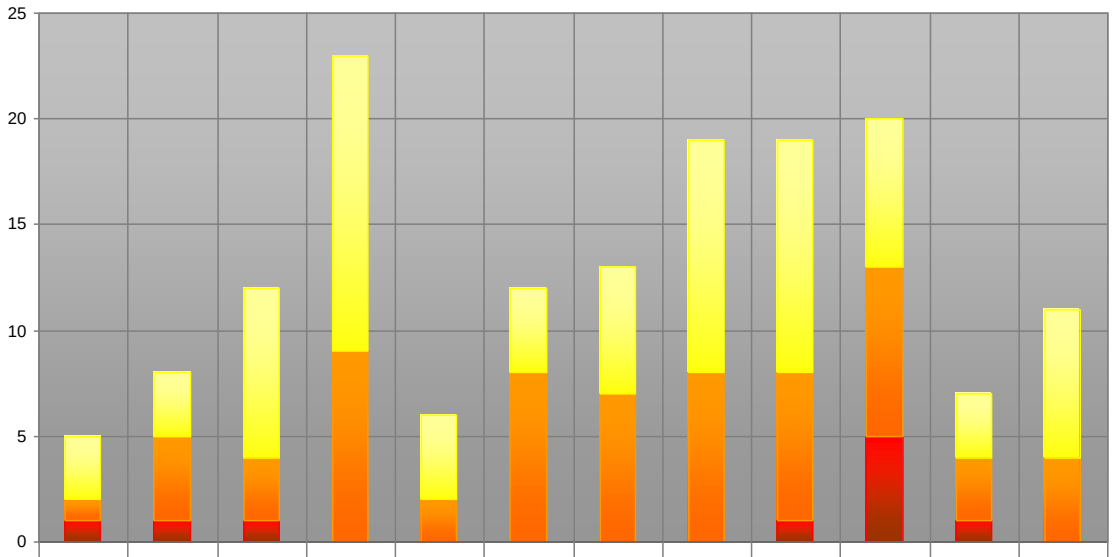
	2010 - Okt	2010 - Nov	2010 - Dez
Cross Site Scripting (XSS)	1		1
Denial of Service (DoS)	1	2	3
Designfehler			1
Directory Traversal			
Eingabeungültigkeit	2		1
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Format String	1		
Konfigurationsfehler			
Pufferüberlauf	13	4	5
Race-Condition	1		
Schwache Authentifizierung			
Schwache			

Verlauf der letzten drei Monate Schwachstelle/Kategorie

© scip AG



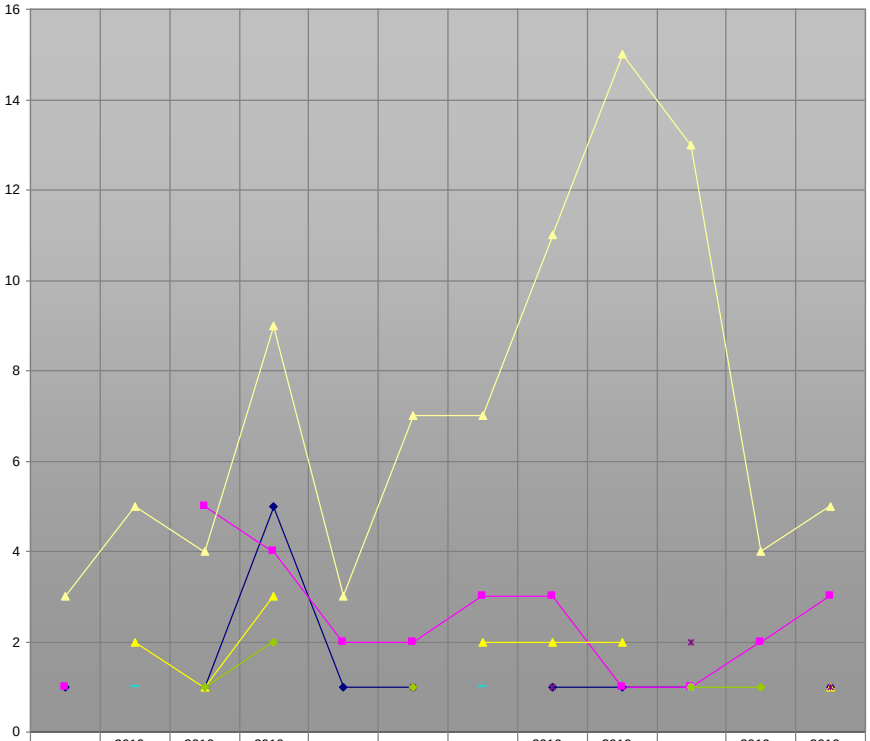
Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2010



	2010 - Jan	2010 - Feb	2010 - Mrz	2010 - Apr	2010 - Mai	2010 - Jun	2010 - Jul	2010 - Aug	2010 - Sep	2010 - Okt	2010 - Nov	2010 - Dez
problematisch	3	3	8	14	4	4	6	11	11	7	3	7
kritisch	1	4	3	9	2	8	7	8	7	8	3	4
sehr kritisch	1	1	1						1	5	1	

Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2010

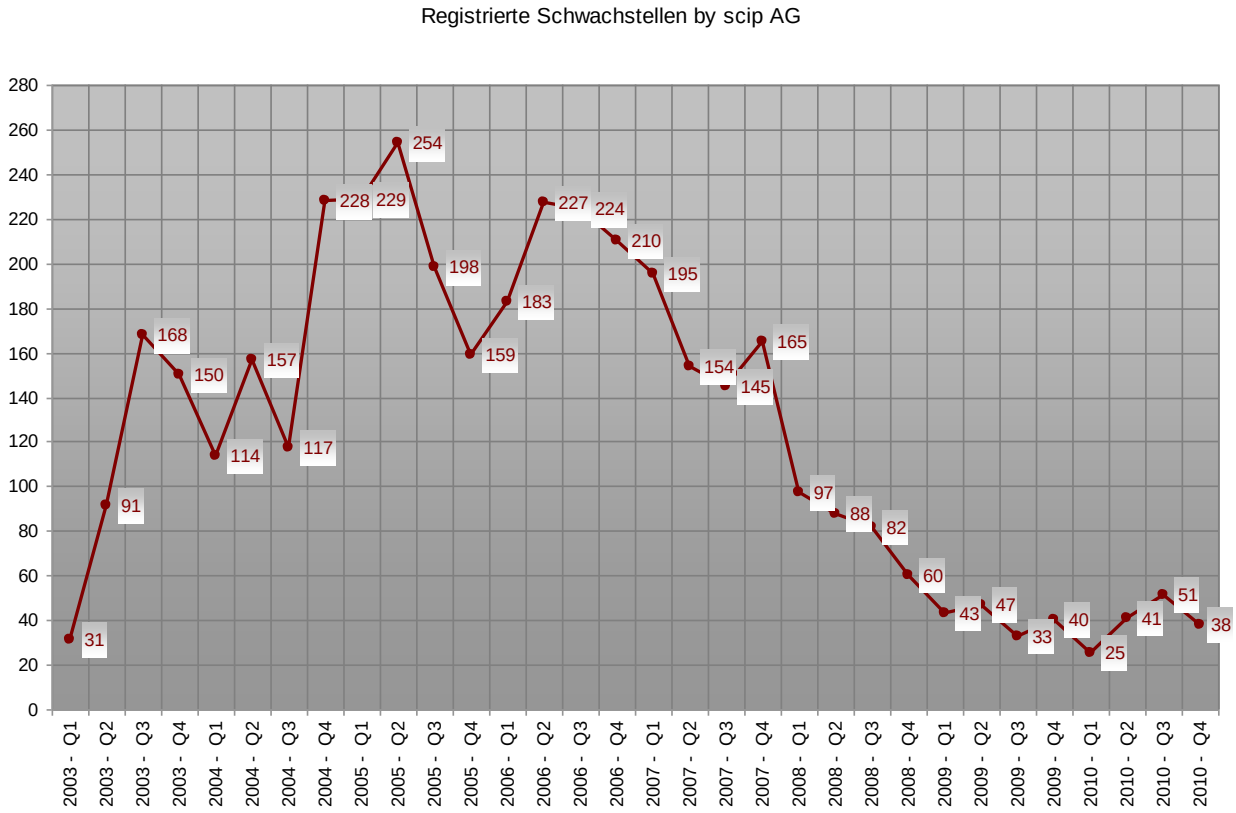
© scip AG



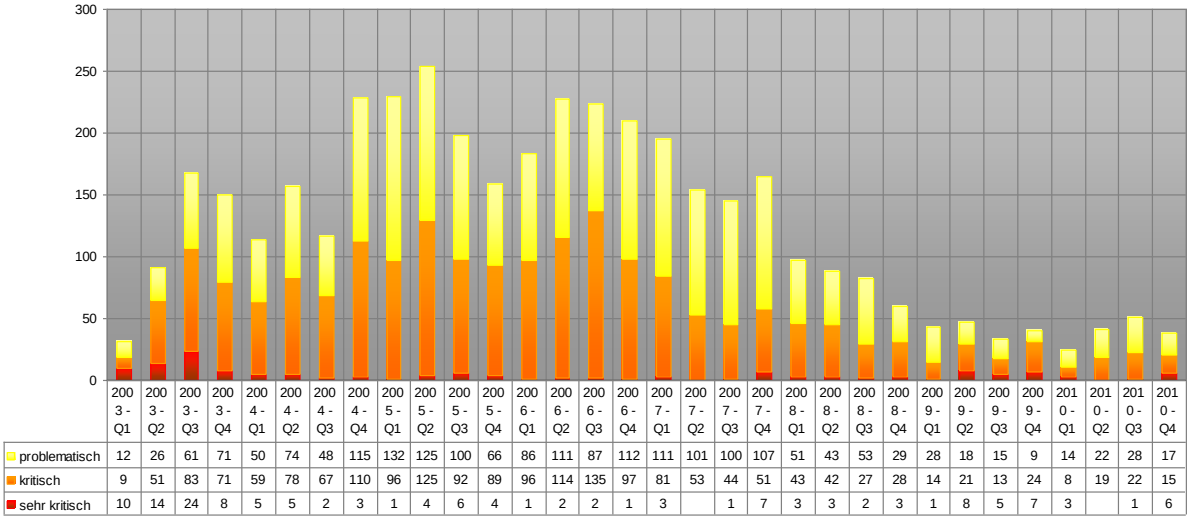
	2010 - Jan	2010 - Feb	2010 - Mrz	2010 - Apr	2010 - Mai	2010 - Jun	2010 - Jul	2010 - Aug	2010 - Sep	2010 - Okt	2010 - Nov	2010 - Dez
Cross Site Scripting (XSS)	1		1	5	1	1		1	1	1		1
Denial of Service (DoS)	1		5	4	2	2	3	3	1	1	2	3
Designfehler		2	1	3			2	2	2			1
Directory Traversal								1				
Eingabeungültigkeit						1		1		2		1
Fehlende Authentifizierung												
Fehlende Verschlüsselung												
Fehlerhafte Leserechte												
Fehlerhafte Schreibrechte												
Format String										1		
Konfigurationsfehler												
Pufferüberlauf	3	5	4	9	3	7	7	11	15	13	4	5
Race-Condition										1		
Schwache Authentifizierung												
Schwache Verschlüsselung												
SQL-Injection												
Symlink-Schwachstelle												
Umgehungs-Angriff		1					1					
Unbekannt			1	2		1				1	1	

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2010

© scip AG



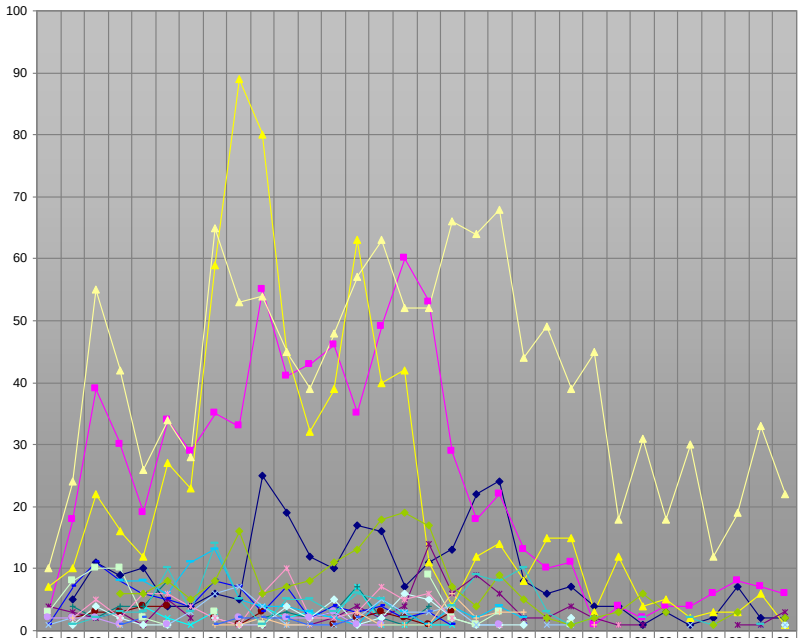
Verlauf der Anzahl Schwachstellen pro Quartal seit Q1/2003



	2003 - Q1	2003 - Q2	2003 - Q3	2003 - Q4	2004 - Q1	2004 - Q2	2004 - Q3	2004 - Q4	2005 - Q1	2005 - Q2	2005 - Q3	2005 - Q4	2006 - Q1	2006 - Q2	2006 - Q3	2006 - Q4	2007 - Q1	2007 - Q2	2007 - Q3	2007 - Q4	2008 - Q1	2008 - Q2	2008 - Q3	2008 - Q4	2009 - Q1	2009 - Q2	2009 - Q3	2009 - Q4	2010 - Q1	2010 - Q2	2010 - Q3	2010 - Q4
problematisch	12	26	61	71	50	74	48	115	132	125	100	66	86	111	87	112	111	101	100	107	51	43	53	29	28	18	15	9	14	22	28	17
kritisch	9	51	83	71	59	78	67	110	96	125	92	89	96	114	135	97	81	53	44	51	43	42	27	28	14	21	13	24	8	19	22	15
sehr kritisch	10	14	24	8	5	5	2	3	1	4	6	4	1	2	2	1	3		1	7	3	3	2	3	1	8	5	7	3		1	6

Verlauf der Anzahl Schwachstellen/Schweregrad pro Quartal seit Q1/2003

© scip AG



	2003-Q1	2003-Q2	2003-Q3	2003-Q4	2004-Q1	2004-Q2	2004-Q3	2004-Q4	2005-Q1	2005-Q2	2005-Q3	2005-Q4	2006-Q1	2006-Q2	2006-Q3	2006-Q4	2007-Q1	2007-Q2	2007-Q3	2007-Q4	2008-Q1	2008-Q2	2008-Q3	2008-Q4	2009-Q1	2009-Q2	2009-Q3	2009-Q4	2010-Q1	2010-Q2	2010-Q3	2010-Q4
Cross Site Scripting (XSS)		5	11	9	10	4	4	6	5	25	19	12	10	17	16	7	11	13	22	24	8	6	7	4	4	1	3	1	2	7	2	2
Denial of Service (DoS)	3	18	39	30	19	34	29	35	33	55	41	43	46	35	49	60	53	29	18	22	13	10	11	1	4	2	4	4	6	8	7	6
Designfehler	7	10	22	16	12	27	23	59	89	80	45	32	39	63	40	42	11	4	12	14	8	15	15	3	12	4	5	2	3	3	6	1
Directory Traversal					4	2	1	3		4	2	3	2	7	1	1	1	1												1		
Eingabeungültigkeit	4	3	2	3	1	5	2		1	1		1	2	4	2	4	14	6	9	6	2	2	4	2	1	1				1	1	3
Fehlende Authentifizierung		2	3	3	4	4		2	1	3			1	2	3	2	1	3														
Fehlende Verschlüsselung		4	2	4	4	8				2	3	2	3	7	2	1	4															
Fehlerhafte Leserechte	1	7	11	8	6	5	4	8	7	3	7	2	4	3	4	2	3	1			1											
Fehlerhafte Schreibrechte				8	8	6	11	13	5	4	4	3	2	1	5	3	1	4	2	4	2											
Format String		1	4	2	1	1		2	1	1	4	2	5	1	2	6	5	2	1	1	1		2									1
Konfigurationsfehler	3	8	10	10	2	1		3		1							9	2	1	3			1									
Pufferüberlauf	10	24	55	42	26	34	28	65	53	54	45	39	48	57	63	52	52	66	64	68	44	49	39	45	18	31	18	30	12	19	33	22
Race-Condition	1	2		1		1	3	6	7	4	1	1	1	2	5	3	3	4	1	1		1	1					1				1
Schwache Authentifizierung		2	5	2	6	6	4	2	1	6	10	2	2	3	7	5	6	2		1					1							
Schwache Verschlüsselung	2	2	2	1		1			2		2	2	3	1	1					1												
SQL-Injection		2		1				1	1	2	1	1		3	1	1	1	6	2	3	3			1								
Symlink-Schwachstelle				1	2			1	2	2	2	1	1	2			3															
Umgehungs-Angriff		1	2	3	3	10	3	14	5	1	5	5	3	6	5	2		4	9	8	10	3	1	2		2		2	1		1	
Unbekannt				6	6	8	5	8	16	6	7	8	11	13	18	19	17	7	4	9	5	2	1	2	3	6	3		1	3		2

Verlauf der Anzahl Schwachstellen/Kategorie pro Quartal seit Q1/2003

© scip AG

5. Labs

Auf der scip Labs Webseite (http://www.scip.ch/?labs.archiv) werden regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

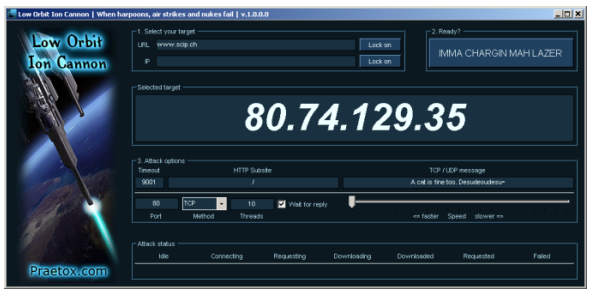
5.1 LOIC-Attacken abwehren - DDoS im Umfeld von Wikileaks

19.12.2010 Marc Ruef, maru@scip.ch

Im Zuge der Festnahme von Julian Assange und dem politischen Druck gegen Wikileaks haben sich verschiedene Kreise zu einer umstrittenen Distributed Denial of Service-Attacke (DDoS) gegen Wikileaks-Gegner zusammengeschlossen. Dieser Operation Payback, die durch Mitglieder des Underground-Forums 4chan orchestriert wird, sind mehrere grosse Dienstleister zum Opfer gefallen:

- EveryDNS
- Paypal
- Postfinance (Details)
- MasterCard
- Visa
- Amazon

Angriffsmechanik
Um diese Angriffe umzusetzen, wird das Tool LOIC (Low Orbit Ion Cannon) verwendet. Dieses wurde ursprünglich in C# geschrieben, ist aber ebenfalls als plattformunabhängige Java-Portierung erhältlich. Es sieht sich in der Lage, das Zielsystem mit einer Vielzahl an Anfragen zu überlasten. Dabei können entweder klassisches TCP- oder UDP-Flooding aber auch HTTP-Flooding durchgesetzt werden.



Der Quelltext der Original-Implementierung steht zur Verfügung und mit der Durchsicht dessen wird die Funktionsweise des Angriffs über HTTP ersichtlich. Diese wird in der Funktion `bw_DoWork()` in der Datei `HTTPFlooder.cs` wie folgt definiert (Zeilen 56-82; letzte Comments leicht gekürzt):

```
private void bw_DoWork(object sender,
DoWorkEventArgs e)
{
   try
   {
      byte[] buf = Sys-
tem.Text.Encoding.ASCII.GetBytes(
         "GET " + Subsite + "
HTTP/1.0\r\n\r\n\r\n");
      IPEndPoint RHost = new IPEnd-
Point(System.Net.IPAddress.Parse(IP),
Port);
      while (isFlooding)
      {
         State = ReqState.Ready; // SET
STATE TO READY //
         LastAction = Tick();
         byte[] recvBuf = new byte[64];
         Socket sck = new Sock-
et(AddressFamily.InterNetwork, Socket-
Type.Stream, ProtocolType.Tcp);
         State = ReqState.Connecting; //
SET STATE TO CONNECTING //
         sck.Connect(RHost);
         sck.Blocking = Resp;
         State = ReqState.Requesting; //
SET STATE TO REQUESTING //
         sck.Send(buf, Socket-
Flags.None);
         State = ReqState.Downloading;
iRequested++; // DOWNLOADING //
REQUESTED++
         if (Resp) sck.Receive(recvBuf,
64, SocketFlags.None);
         State = ReqState.Completed;
iDownloaded++; // COMPLETED //
DOWNLOADED++
         if (Delay>0) Sys-
tem.Threading.Thread.Sleep(Delay);
      }
   }
   catch { }
   isFlooding = false;
}
```

Gegenmassnahmen
Hierbei ist zu sehen, wie in der Variable `buf` die HTTP GET-Anfrage definiert wird. Diese weist drei Auffälligkeiten auf:

1. Es wird lediglich `HTTP/1.0` (und kein HTTP/1.1) unterstützt.
2. Somit wird keine in HTTP/1.1 obligatorische Host-Zeile mitgeschickt.
3. Die Anfrage wird mit *drei* anstelle von den nur erforderlichen zwei `\r\n` abgeschlossen.

Diese drei Eigenschaften machen es möglich, derlei Zugriffe erkennen und frühstmöglich mitigieren zu können. Vor allem das letztgenannte Detail ist unüblich bei herkömmlichen GET-Anfragen. Ein entsprechendes Unterdrücken mit einem Proxy-Element oder einem `.htaccess/mod_security` Filter können da-

© scip AG

bei helfen, die Wucht der sehr primitiven Attacke abzufedern.

Zudem unterstützen die gegenwärtigen Versionen von LOIC keinerlei Möglichkeit zum Spoofing der Quell-IP-Adressen oder dem Generieren von Decoy-Zugriffen (diese wären vor allem im UDP-Modus effektiv). Aus diesem Grund kann es auch einfach nur helfen, mittels einem Protocol Analyzer die Zugriffe mitzulesen und in periodischer Weise restriktive IP-Filter für die einzelnen DDoS-Nodes anzuwenden (einfaches Beispiel mit .htaccess). Der LOIC-Client wird von den meisten Antiviren-Lösungen als solcher erkannt.

Weitere Informationen zum Schutz gegen DDoS-Attacken fasst die hervorragende Arbeit A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms zusammen. Eine Diskussion zur Entwicklung von Gegenmassnahmen in den letzten 10 Jahren ist auf der Mailingliste der NANOG zu finden.

6. Impressum

Herausgeber:

)SCIP(scip ag
scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
mailto:info@scip.ch
http://www.scip.ch

Zuständige Person:

Marc Ruef
Security Consultant
T +41 44 404 13 13
mailto:maru@scip.ch

scip AG ist eine unabhängige Aktiengesellschaft mit Sitz in Zürich. Seit der Gründung im September 2002 fokussiert sich die scip AG auf Dienstleistungen im Bereich Information Security. Unsere Kernkompetenz liegt dabei in der Überprüfung der implementierten Sicherheitsmassnahmen mittels **Penetration Tests** und **Security Audits** und der Sicherstellung zur Nachvollziehbarkeit möglicher Eingriffsversuche und Attacken (**Log-Management** und **Forensische Analysen**). Vor dem Zusammenschluss unseres spezialisierten Teams waren die meisten Mitarbeiter mit der Implementierung von Sicherheitsinfrastrukturen beschäftigen. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, TrendMicro, Symantec etc.), welche den Grundstein für unsere Projekte bilden. Das Grundwissen vervollständigen unsere Mitarbeiter durch ihre ausgeprägten Programmierkenntnisse. Dieses Wissen äussert sich in selbst geschriebenen Routinen zur Ausnutzung gefundener Schwachstellen, dem Coding einer offenen Exploiting- und Scanning Software als auch der Programmierung eines eigenen Log-Management Frameworks. Den kleinsten Teil des Wissens über Penetration Test und Log-Management lernt man jedoch an Schulen – nur jahrelange Erfahrung kann ein lückenloses Aufdecken von Schwachstellen und die Nachvollziehbarkeit von Angriffsversuchen garantieren.

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