)SCIP(

scip ag

Contents

1. Editorial

Der Verfasservertrag - Tipps für Autoren

Vor einiger Zeit wurde ich vom Herausgeber eines Buchs zum Thema Informationssicherheit angefragt, ob ich der anstehenden Neuauflage einen Beitrag beisteuern möchte. Als Thema hatte er für mich Sicherheit im Cloud Computing vorgesehen, wobei ihm voraussichtlich meine Auflistung der 10 sicherheitsrelevanten Gründe gegen Cloud Computing gefallen hat.

Ich habe eingewilligt und mich ans Schreiben gemacht (ich bin stets jemand, der frühzeitig mit einer Auftragsarbeit fertig ist). Währenddessen sollte das Vertragswerk zur Gegenzeichnung bei mir eintreffen. Im sogenannten Verfasservertrag werden die Rechten und Pflichten zwischen Autor und Verlag definiert. Ich habe schon so manchen Autorenvertrag gesehen und fast die meisten davon teilweise oder ganz abweisen müssen.

Dabei sind folgende Punkte meines Erachtens aus der Sicht eines Autors besonders wichtig. Diese sind als Empfehlung für jeden zu sehen, der gerne bei einem Verlag einen Fachbeitrag oder ein Buch auflegen möchte:

* Definition des Honorars: Es muss eine klare Regelung bezüglich des Honorars stattfinden. Im Idealfall erhält der Autor als erstes ein verkaufsunabhängiges Initialhonorar. Zusätzlich erhält er ebenso - in der Regel Buchverkäufen vorenthalten - eine Umsatzbeteiligung.

* Nennung des Autors: Ein Autor soll und darf darauf bestehen, dass er im Rahmen der Veröffentlichung des Werks als dessen Urheber genannt wird. Diese Nennung ist nicht nur auf die Vertragsdauer bzw. Dauer der Zusammenarbeit festzulegen. Stattdessen ist diese für die gesamte Zeitdauer der Nutzung und des Vertriebs des Werks einzuhalten.

* Zeitdauer der Nutzungsrechte: Die Zeitdauer des Nutzungsrechte durch den Vertrag ist bestmöglich festzulegen. Dabei kann sich auf eine Auflage oder auf einen Zeitraum geeinigt werden. Hierbei gilt es zu definieren, was nach Ablauf dieser Zeitdauer - vor allem mit den Nutzungsrechten - genau geschieht.

* Anpassungen und Korrekturen: Verlage wollen in der Regel Anpassungen, Korrekturen und Erweiterungen durch den Autor vornehmen lassen. Dies ist zum Beispiel dann der Fall, wenn eine Neuauflage eines Buchs geplant ist. Hierbei gilt es ebenso zu definieren, ob und inwiefern solche Anpassungen vom Verlag durchgesetzt und durch den Autor berücksichtigt werden müssen. Im Idealfall kann der Autor auf die Umsetzung unliebsamer Anpassungen verzichten.

* Weiterverarbeitung durch Dritte: Will oder kann ein Autor nicht mehr mit einem Verlag zusammenarbeiten, muss definiert werden, inwiefern Dritte die gewünschten Anpassungen vornehmen können lassen sollen. Auf eine unerlaubte Anpassung des Originalwerks sollte verzichtet werden.

* Rückgabe der Nutzungsrechte: Im Vertragswerk sollte festgehalten werden, wann und wie die Rechte an den Autor zurückgehen. Dies ist zum Beispiel dann der Fall, wenn ein Buch nicht mehr aufgelegt wird oder x Jahre nach dem Erscheinen eines Fachartikels. Mit der Rückgabe der Nutzungsrechte sollte der Autor wieder frei über sein Erzeugnis verfügen können. Dies schliesst die Anpassung und den Weiterverkauf mit ein.

* Wiederruf der Nutzungsrechte: Einem Autor sollte es stets vorbehalten sein, die an den Verlag gewährten Nutzungsrechte zu widerrufen. Dies kann auf wirtschaftliche Unstimmigkeiten

oder bei einem partiellen Vertragsbruch der Fall sein.

Die meisten Verlage sind, gerade bei einem Erstlingswerk eines Autoren, gar nicht begeistert von diesen Forderungen. In praktisch allen Punkten ist der Verlag nämlich darum bemüht, dass er den gesamten Handlungsspielraum für sich alleine in Anspruch nehmen kann.

Setzt man als Autor entsprechenden Druck auf, um seine eigenen Rechte aufrecht erhalten zu können, muss man mit einem Rückzug des Verlags rechnen.

So auch im geschilderten Fall, in dem der Verlag in keinem Punkt meinen Forderungen einwilligen konnte. Eine Zusammenarbeit ist deshalb nicht zustande gekommen.

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 11. Juli 2011

2. scip AG Informationen

2.1 Evidence Collection

Umfangreiche, integre und nachvollziehbare Sammlung und Sicherung von Daten als Grundlage für eine forensische Analyse.

- Vorbereitung: Grundlegende Informationen zum Incident, den betroffenen Komponenten sowie den zu sammelnden Daten werden eingeholt.
- Datensicherung: Die Integrität der Daten sowie der betroffenen Objekte wird vor, während und nach der Datensammlung gewährleistet (z.B. Erstellung von Backup, Arbeit nur mit Kopie).
- Datensammlung: Die Daten werden aus den betroffenen Objekten in sicherer und nachvollziehbarer Weise extrahiert (z.B. ständige Protokollierung, keine invasiven Zugriffe).

Der Kunde erhält ein Dokument, welches das Vorgehen der Datensammlung sowie die zusammengetragenen Daten protokolliert. Ebenso werden die extrahierten Daten auf einem Datenträger zur Verfügung gestellt.

Eine integre und nachvollziehbare Datensammlung und Spurensicherung ist unabdingbar, um eine effektive forensische Untersuchung durchführen zu können (siehe Forensic Analysis). Das erfolgreiche Umsetzen einer Evidence Collection und Preservation ist jenachdem mit gewissem Aufwand verbunden.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen haben wir als scip AG bereits eine Vielzahl von Forensik-Projekten durchgeführt.

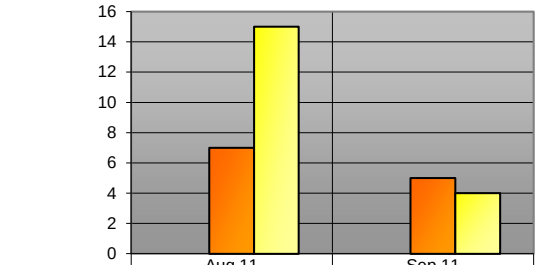
Zählen auch Sie auf uns!
http://www.scip.ch/?firma.referenzenalle

Zögern Sie nicht und kontaktieren Sie unseren Herrn Simon Zumstein unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an simon.zumstein@scip.ch.

3. Neue Sicherheitslücken

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

Das Dienstleistungspaket VulDB Alert System liefern Ihnen jene Informationen, die genau für Ihre Systeme relevant sind: http://www.scip.ch/?vuldb.alertsystem



	Aug 11	Sep 11
sehr kritisch	0	0
kritisch	7	5
problematisch	15	4

Inhalt

3.1 Linux Kernel CIFS DFS Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 15.09.2011
VulDB: http://www.scip.ch/?vuldb.4416

Linux ist ein Betriebssystemkern (engl. kernel). Er wurde im Jahr 1991 von dem Finnen Linus Torvalds ursprünglich für die x86-Architektur entwickelt und unter der freien GNU General Public License (GPL) veröffentlicht. Der Kern (Kernel) findet in einer Vielzahl von Distributionen und Betriebssystemen seine Anwendung. Shogesh Sharma identifizierte unlängst eine Denial of Service Verwundbarkeit in aktuellen Versionen des Produktes. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und - unter bislang nicht gesicherten Umständen - beliebigen Code zur Ausführung bringen.

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

3.2 Adobe Reader/Acrobat verschiedene Schwachstellen

Risiko: kritisch
Remote: Ja
Datum: 14.09.2011
VulDB: http://www.scip.ch/?vuldb.4415

Unter Adobe Acrobat wird eine Gruppe von Programmen zusammengefasst, die zum Erstellen, Verwalten, Kommentieren und Verteilen von PDF-Dateien verwendet werden. Dieses kostenpflichtige Programmpaket des Software-Unternehmens Adobe Systems enthält ein Anwendungsprogramm zum Erstellen und Bearbeiten von PDF-Dokumenten. Adobe bietet in seiner Acrobat-Familie weitgehende Unterstützung von digitalen Unterschriften (Signaturen) und grundsätzliche Unterstützung von Verschlüsselungstechnologien. Ein Kollektiv von Researchern (siehe Original Advisory für Credits) identifizierte diverse Schwachstellen in aktuellen Versionen des Produktes. Die gelisteten Schwachstellen sind teilweise als kritisch zu betrachten und können teilweise zur kompletten Kompromittierung des Zielsystems führen.

Expertenmeinung:

Die vorliegenden Schwachstellen sind als teilweise kritisch zu betrachten und sollten zeitnah durch das Einspielen entsprechender kumulativer Patchpakete oder individueller Patches mitigiert werden.

3.3 Microsoft SharePoint Cross-Site Scripting Schwachstelle

Risiko: problematisch
Remote: Ja
Datum: 13.09.2011
VulDB: http://www.scip.ch/?vuldb.4414

Bei SharePoint handelt es sich um die Kurzbezeichnung für einen Verbund von Software-Produkten der Firma Microsoft. SharePoint ist eher eine Plattform als eine Anwendung für einen bestimmten Zweck. Aufgrund des großen Funktionsumfangs wird SharePoint für die unterschiedlichsten Zwecke in den Unternehmen eingesetzt, beispielsweise als Mitarbeiter- oder Unternehmensportal, als Informationsportal für das Berichtswesen oder als Dokumentenmanagementsystem. Ein Kollektiv von Researchern (siehe Original Advisory für Credits) veröffentlichte unlängst verschiedene Schwachstellen, vornehmlich der Kategorie Cross Site Scripting (XSS) in verschiedenen Versionen des Produktes. Die gelisteten Schwachstellen sind teilweise als kritisch zu betrachten und können teilweise zur kompletten Kompromittierung des Zielsystems führen.

Expertenmeinung:
Die vorliegenden Schwachstellen sind als teilweise kritisch zu betrachten und sollten zeitnah durch das Einspielen entsprechender kumulativer Patchpakete oder individueller Patches mitigiert werden.

3.4 Microsoft SharePoint XML/XSL Processing File Disclosure Schwachstelle

Risiko: problematisch
Remote: Ja
Datum: 13.09.2011
VulDB: http://www.scip.ch/?vuldb.4413

Microsoft Office ist das Office-Paket des US-amerikanischen Unternehmens Microsoft für die Betriebssysteme Microsoft Windows und Mac OS X. Für unterschiedliche Aufgabenstellungen werden verschiedene Suiten angeboten, die sich in den enthaltenen Komponenten, dem Preis und der Lizenzierung unterscheiden. Der Researcher Nicolas Grégoire der Firma Agarri veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Designfehler) 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 Office Insecure Library Loading Schwachstelle

Risiko: kritisch
Remote: Ja
Datum: 13.09.2011
VulDB: http://www.scip.ch/?vuldb.4412

Microsoft Office ist das Office-Paket des US-amerikanischen Unternehmens Microsoft für die Betriebssysteme Microsoft Windows und Mac OS X. Für unterschiedliche Aufgabenstellungen werden verschiedene Suiten angeboten, die sich in den enthaltenen Komponenten, dem Preis und der Lizenzierung unterscheiden. Ein Kollektiv von Researchern (David Warren, Parvez Anwar) identifizierte diverse Schwachstellen in aktuellen Versionen des Produktes. Die gelisteten Schwachstellen sind teilweise als kritisch zu betrachten und können teilweise zur kompletten Kompromittierung des Zielsystems führen.

Expertenmeinung:
Die vorliegenden Schwachstellen sind als teilweise kritisch zu betrachten und sollten zeitnah durch das Einspielen entsprechender kumulativer Patchpakete oder individueller Patches mitigiert werden.

3.6 Microsoft Office Excel verschiedene Schwachstellen

Risiko: kritisch
Remote: Ja
Datum: 13.09.2011
VulDB: http://www.scip.ch/?vuldb.4411

Microsoft Excel ist das am weitesten verbreitete Tabellenkalkulationsprogramm. Excel gehört zur Microsoft-Office-Suite und ist sowohl für Microsoft Windows als auch für Mac OS verfügbar. Excel entstand als Nachfolger von Microsoft Multiplan. Die aktuelle Version ist für Windows Microsoft Excel 2010 und für Mac OS Microsoft Excel 2011. Ein Kollektiv von Researchern (siehe Original Advisory für Credits) identifizierte diverse Schwachstellen in aktuellen Versionen des Produktes. Die gelisteten Schwachstellen sind teilweise als kritisch zu

betrachten und können teilweise zur kompletten Kompromittierung des Zielsystems führen.

Expertenmeinung:
Die vorliegenden Schwachstellen sind als teilweise kritisch zu betrachten und sollten zeitnah durch das Einspielen entsprechender kumulativer Patchpakete oder individueller Patches mitigiert werden.

3.7 Microsoft Windows Insecure Library Loading Schwachstelle

Risiko: kritisch
Remote: Ja
Datum: 13.09.2011
VulDB: http://www.scip.ch/?vuldb.4410

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 die Benutzeroberfläche von Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Die Firma ACROS Security identifizierte unlängst eine Schwachstelle (Designfehler) in aktuellen Versionen der vorliegenden 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.

3.8 Microsoft Windows WINS Privilege Escalation

Risiko: problematisch
Remote: Ja
Datum: 13.09.2011
VulDB: http://www.scip.ch/?vuldb.4409

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 die Benutzeroberfläche von Anwendungen als rechteckige Fenster auf dem Bildschirm dargestellt werden. Der Researcher Nicolas Economou der Firma Core Security veröffentlichte unlängst ein Advisory, indem er eine Schwachstelle (Designfehler) in verschiedenen Versionen des Produktes beschreibt. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

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

3.9 Siemens SIMATIC WinCC Flexible Tag Simulator Memory Corruption

Risiko: kritisch
Remote: Ja
Datum: 01.09.2011
VulDB: http://www.scip.ch/?vuldb.4408

WinCC (Windows Control Center) ist ein PC-basiertes Prozessvisualisierungssystem der Firma Siemens. Es wird als eigenständiges SCADA-System oder als Mensch-Maschine-Schnittstelle für Prozessleitsysteme wie SIMATIC PCS7 oder Spectrum PowerCC eingesetzt. Die Software wurde 1996 in der Version 1.1 erstmals im deutschsprachigen Raum breit vermarktet. Ein Researcherteam des ICS-CERT bestehend aus Billy Rios und Terry McCorkle identifizierte unlängst einen Pufferüberlauf in aktuellen Versionen des Produktes. Diese Schwäche erlaubt es einem Angreifer, Kontroller über das System zu erlangen und seine Rechte zu erweitern.

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

3.10 Squid Gopher Response Processing Pufferüberlauf

Risiko: kritisch
Remote: Ja
Datum: 29.08.2011
VulDB: http://www.scip.ch/?vuldb.4407

Squid ist der Name eines freien Proxyservers, der unter der GNU General Public Licence steht. Er zeichnet sich vor allem durch seine gute Skalierbarkeit aus. Squid unterstützt die Netzwerkprotokolle HTTP/HTTPS, FTP über HTTP und Gopher. Ben Hawkes (Google

Security Team) beschreibt eine Pufferüberlauf-Schwachstelle in aktuellen Produktversionen. 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.

3.11 Linux Kernel CIFSFindNext() Signedness Error Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 24.08.2011
VulDB: http://www.scip.ch/?vuldb.4406

Linux ist ein Betriebssystemkern (engl. kernel). Er wurde im Jahr 1991 von dem Finnen Linus Torvalds ursprünglich für die x86-Architektur entwickelt und unter der freien GNU General Public License (GPL) veröffentlicht. Der Kern (Kernel) findet in einer Vielzahl von Distributionen und Betriebssystemen seine Anwendung. Der Researcher Darren Lavender identifizierte unlängst eine Denial of Service Verwundbarkeit in aktuellen Versionen des Produktes. Durch die Ausnutzung der Schwachstelle kann ein Angreifer einen Denial of Service Angriff erzeugen und - unter bislang nicht gesicherten Umständen - beliebigen Code zur Ausführung bringen.

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

3.12 Citrix Access Gateway unspezifizierte Cross-Site Scripting Schwachstelle

Risiko: problematisch
Remote: Ja
Datum: 24.08.2011
VulDB: http://www.scip.ch/?vuldb.4405

Die Citrix Systems, Inc. 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. Die Firma Citrix Systems 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:
Die vorliegenden Schwachstellen sind als teilweise kritisch zu betrachten und sollten zeitnah durch das Einspielen entsprechender kumulativer Patchpakete oder individueller Patches mitigiert werden.

3.13 Cisco IOS SSH2 Sessions Denial of Service

Risiko: problematisch
Remote: Ja
Datum: 23.08.2011
VulDB: http://www.scip.ch/?vuldb.4404

Internetwork Operating System Software (IOS) ist das Betriebssystem von Cisco-Routern und -Switches. Das Betriebssystem geht zurück auf den Angestellten der Stanforder Medizinischen Schule namens Bill Yeager, der um 1980 die Software entwickelte, welche es den Routern ermöglicht, Netzwerke unterschiedlicher Medien und Protokolle miteinander zu verbinden. Er arbeitete bis 1984 mit Sandra Lerner und Len Boseck, den Gründern von Cisco, an der Verbesserung dieser Software zusammen. Mit der Gründung von Cisco im Jahre 1984 lizenzierte Cisco diese Software von Yeager. Seitdem wurde sie in verschiedenen Versionen eingesetzt und liegt seit Oktober 2009 in der Version 15.0 vor. Die Firma Cisco identifizierte unlängst eine Denial of Service Verwundbarkeit in aktuellen 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:
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.

3.14 Google Chrome verschiedene Schwachstellen

Risiko: kritisch
Remote: Ja
Datum: 23.08.2011

VulDB: http://www.scip.ch/?vuldb.4403

Google Chrome ist ein Webbrowser, der von Google Inc. entwickelt wird und seit dem 2. September 2008 verfügbar ist. Am 11. Dezember 2008 erschien die erste finale Version. Zentrales Konzept ist die Aufteilung des Browsers in optisch und auf Prozessebene getrennte Browser-Tabs. Ein Kollektiv von Researchern (siehe Original Advisory für Credits) identifizierte diverse Schwachstellen in aktuellen Versionen des Produktes. Die gelisteten Schwachstellen sind teilweise als kritisch zu betrachten und können teilweise zur kompletten Kompromittierung des Zielsystems führen.

Expertenmeinung:
Die vorliegenden Schwachstellen sind als teilweise kritisch zu betrachten und sollten zeitnah durch das Einspielen entsprechender kumulativer Patchpakete oder individueller Patches mitigiert werden.

3.15 Pidgin verschiedene Schwachstellen

Risiko: problematisch
Remote: Ja
Datum: 22.08.2011
VulDB: http://www.scip.ch/?vuldb.4402

Pidgin (früher Gaim, nicht zu verwechseln mit Gajim) ist ein freier Multi-Protokoll-Client, der von Mark Spencer ursprünglich für unixähnliche Systeme (Linux, BSD) geschrieben wurde, inzwischen aber auch auf Microsoft Windows lauffähig ist und mit Plug-ins stark erweitert werden kann. Ein Kollektiv von Researchern (siehe Original Advisory für Credits) identifizierte diverse Schwachstellen in aktuellen Versionen des Produktes. Die gelisteten Schwachstellen sind teilweise als kritisch zu betrachten und können teilweise zur kompletten Kompromittierung des Zielsystems führen.

Expertenmeinung:
Die vorliegenden Schwachstellen sind als teilweise kritisch zu betrachten und sollten zeitnah durch das Einspielen entsprechender kumulativer Patchpakete oder individueller Patches mitigiert werden.

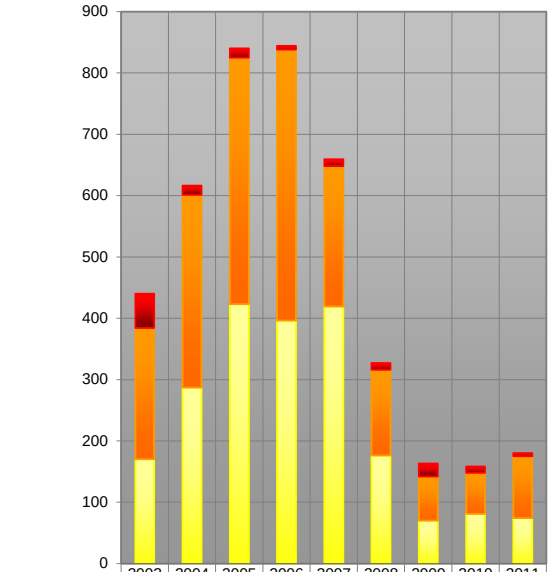
4. Statistiken Verletzbarkeiten

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

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

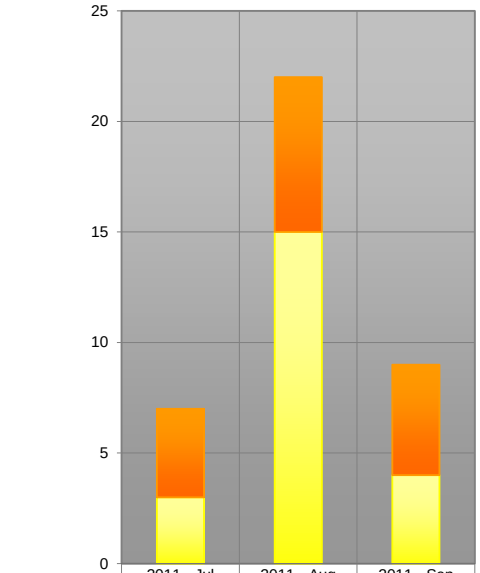
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an info-at-scip.ch. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum:	19. September 2011



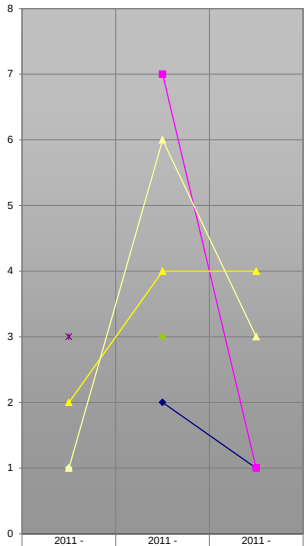
	2003	2004	2005	2006	2007	2008	2009	2010	2011
sehr kritisch	56	15	15	6	11	11	21	10	5
kritisch	214	314	402	442	229	140	72	67	101
problematisch	170	287	423	396	419	176	70	81	74

Verlauf der Anzahl Schwachstellen pro Jahr



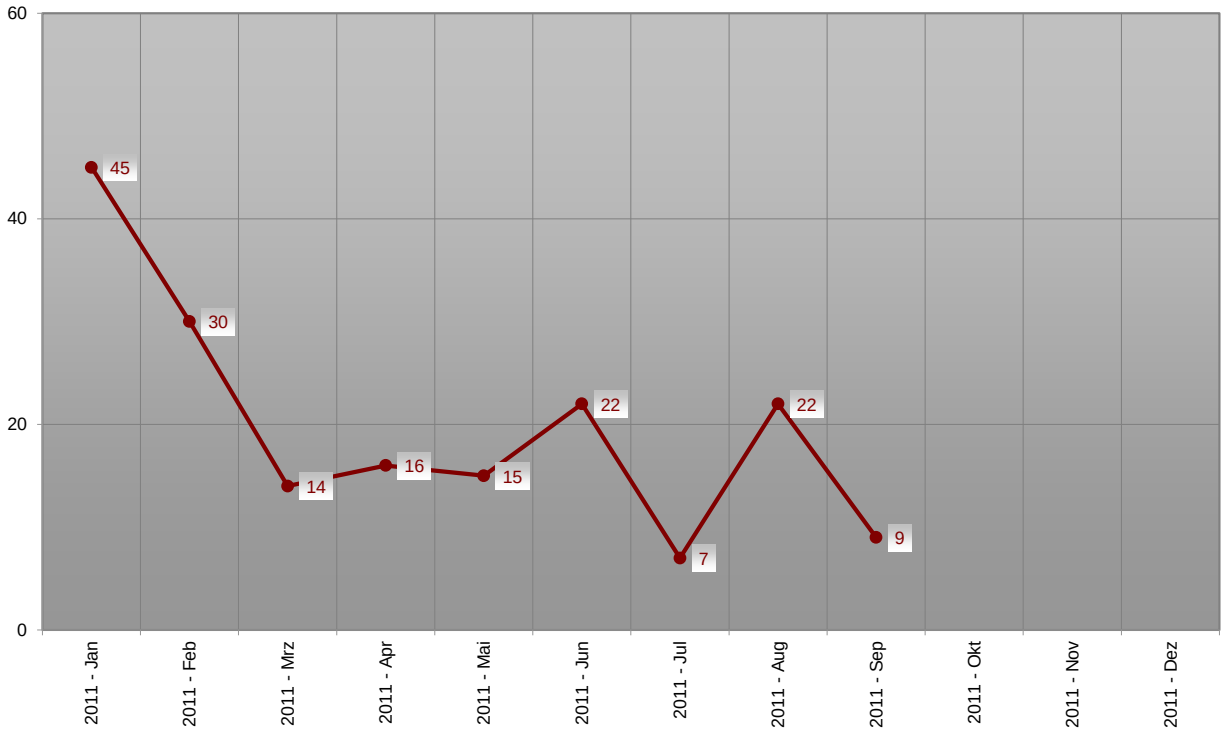
	2011 - Jul	2011 - Aug	2011 - Sep
sehr kritisch			
kritisch	4	7	5
problematisch	3	15	4

Verlauf der letzten drei Monate Schwachstelle/Schweregrad

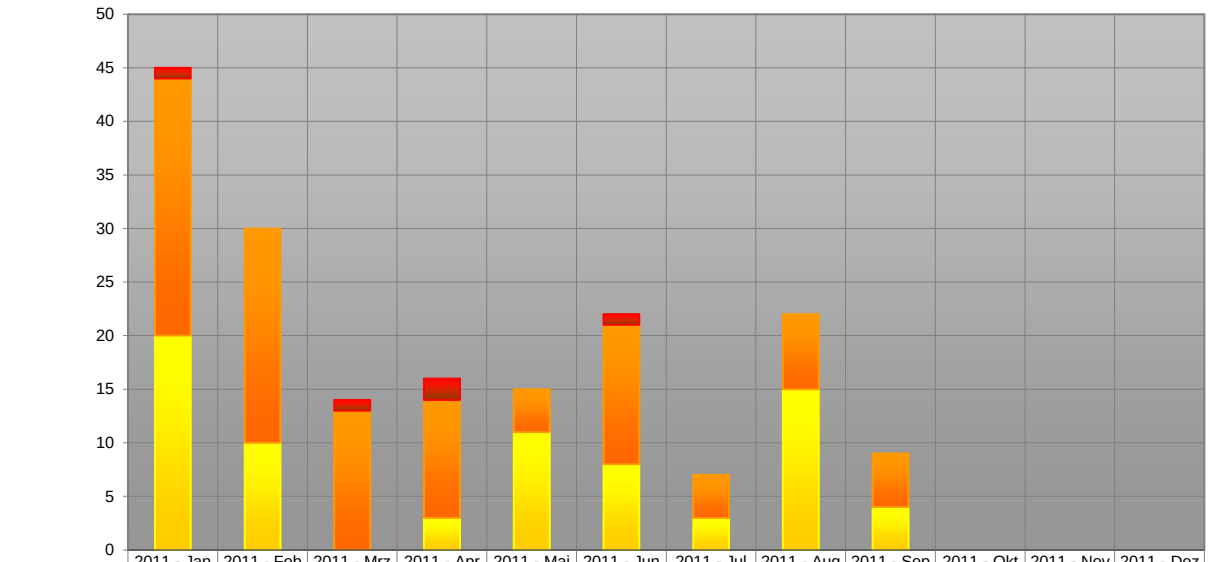


	2011 - Jul	2011 - Aug	2011 - Sep
Cross Site Scripting (XSS)		2	1
Denial of Service (DoS)		7	1
Designfehler	2	4	4
Directory Traversal			
Eingabeungültigkeit	3		
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Format String	1		
Konfigurationsfehler			
Pufferüberlauf	1	6	3
Race-Condition			
Schwache Authentifizierung			
Schwache Verschlüsselung			
SQL-Injection			
Symlink-Schwachstelle			
Umgehungs-Angriff			
Unbekannt		3	

Verlauf der letzten drei Monate Schwachstelle/Kategorie

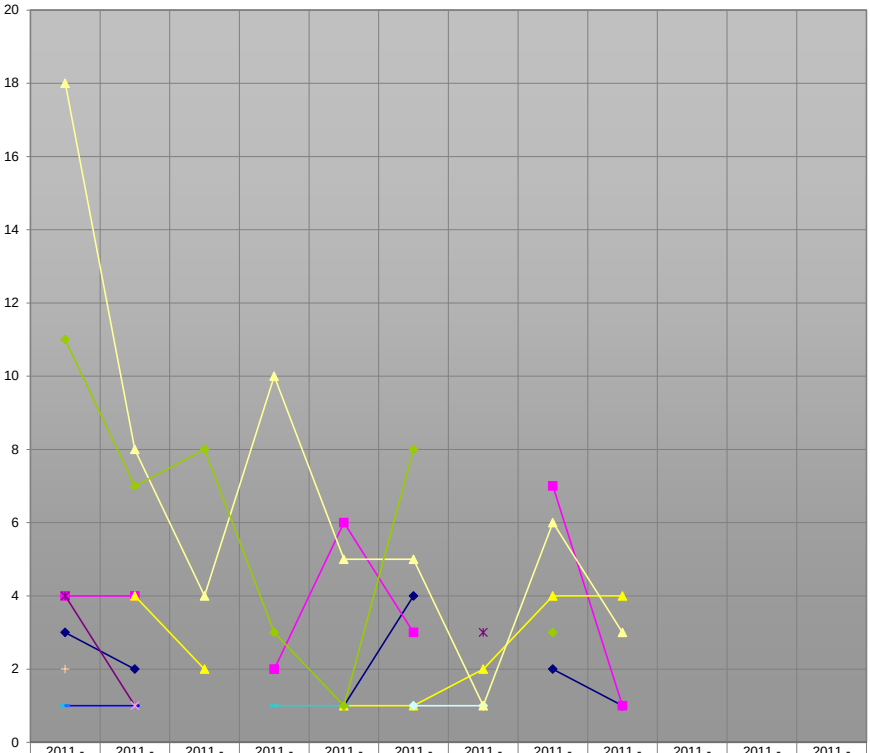


Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2011



	2011 - Jan	2011 - Feb	2011 - Mrz	2011 - Apr	2011 - Mai	2011 - Jun	2011 - Jul	2011 - Aug	2011 - Sep	2011 - Okt	2011 - Nov	2011 - Dez
sehr kritisch	1		1	2		1						
kritisch	24	20	13	11	4	13	4	7	5			
problematisch	20	10		3	11	8	3	15	4			

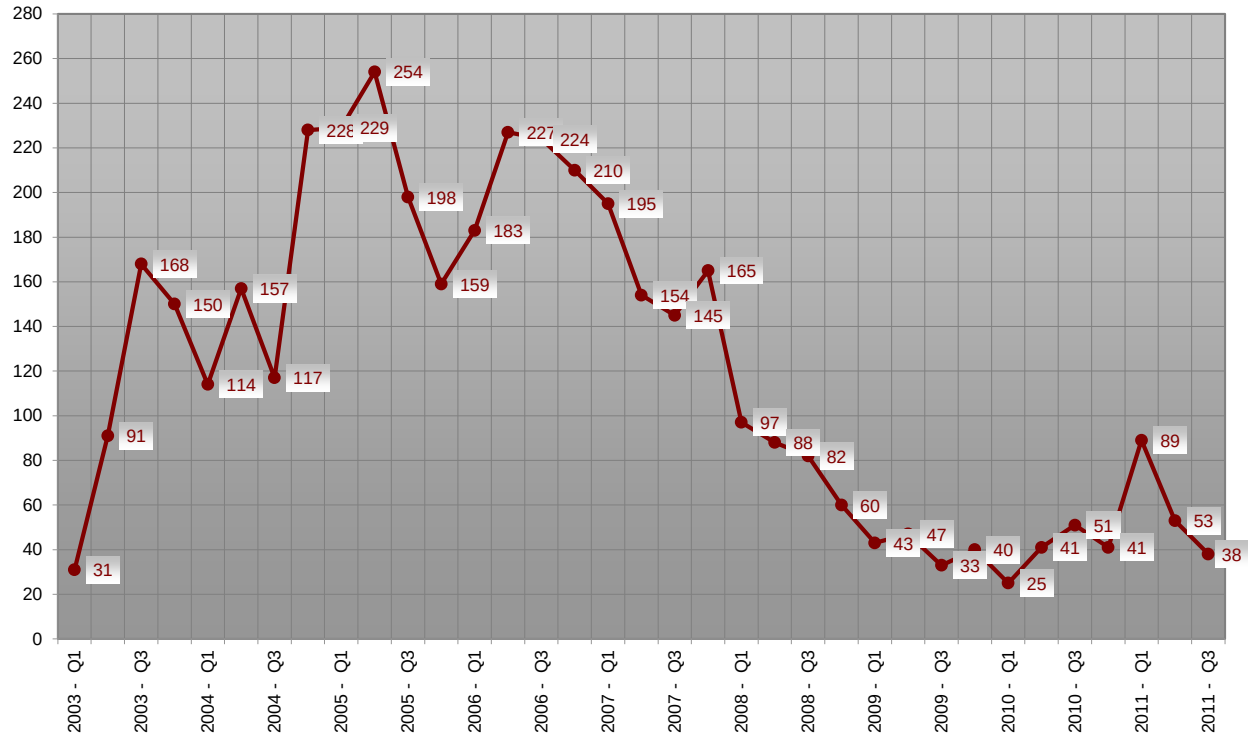
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2011



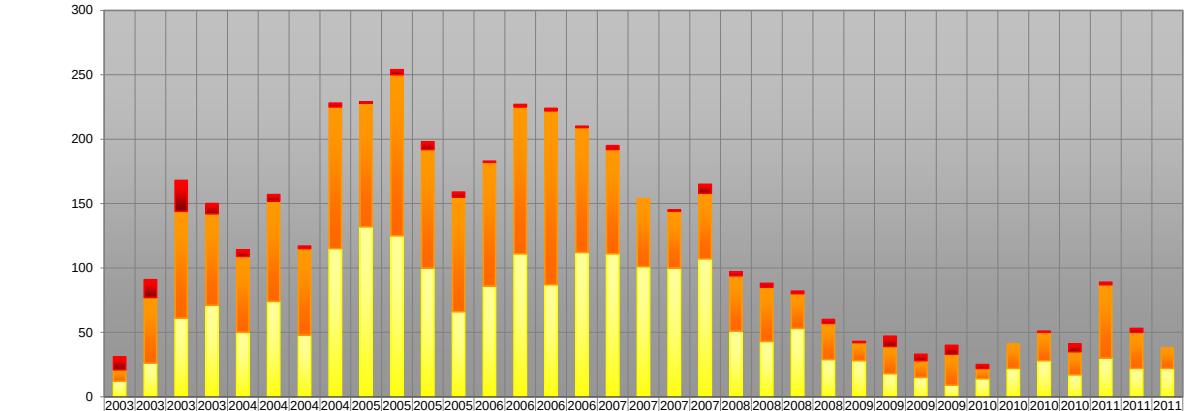
	2011 - Jan	2011 - Feb	2011 - Mrz	2011 - Apr	2011 - Mai	2011 - Jun	2011 - Jul	2011 - Aug	2011 - Sep	2011 - Okt	2011 - Nov	2011 - Dez
Cross Site Scripting (XSS)	3	2			1	4		2	1			
Denial of Service (DoS)	4	4		2	6	3		7	1			
Designfehler		4	2		1	1	2	4	4			
Directory Traversal		1										
Eingabeungültigkeit	4	1					3					
Fehlende Authentifizierung												
Fehlende Verschlüsselung												
Fehlerhafte Leserechte	1	1										
Fehlerhafte Schreibrechte	1											
Format String						1	1					
Konfigurationsfehler												
Pufferüberlauf	18	8	4	10	5	5	1	6	3			
Race-Condition		1										
Schwache Authentifizierung		1										
Schwache Verschlüsselung												
SQL-Injection	2											
Symlink-Schwachstelle	1											
Umgehungs-Angriff				1	1							
Unbekannt	11	7	8	3	1	8		3				

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2011

Registrierte Schwachstellen by scip AG

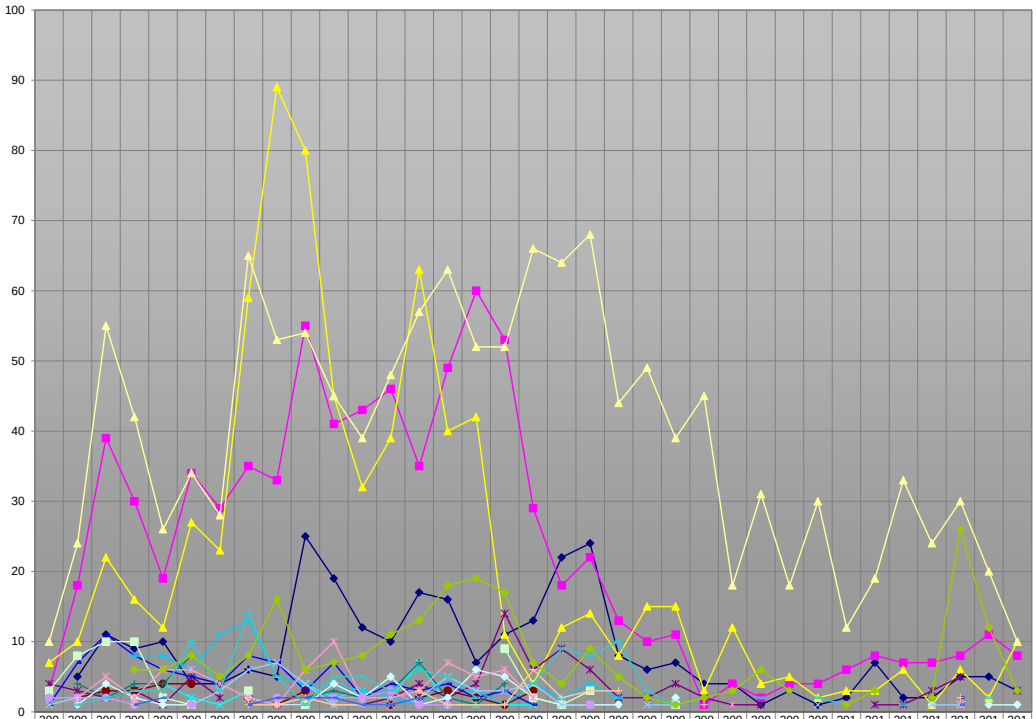


Verlauf der Anzahl Schwachstellen pro Quartal seit Q1/2003



	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	2011 - Q1	2011 - Q2	2011 - Q3
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	2	3	
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	18	57	28	16
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	30	22	22

Verlauf der Anzahl Schwachstellen/Schweregrad 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	2011-Q1	2011-Q2	2011-Q3
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	5	5	3
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	7	8	11	8
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	6	2	10
Directory Traversal					4	2	1	3		4	2	3	2	7	1	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	5		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												2		
Fehlerhafte Schreibrechte				8	8	6	11	13	5	4	4	3	2	1	5	3	1	4	2	4	2												1		
Format String		1	4	2	1	1		2	1	1	4	2	5	1	2	6	5	2	1	1	1		2									1		1	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	24	30	20	10
Race-Condition	1	2		1		1	3	6	7	4	1	1	1	2	5	3	3	4	1	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								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									2		
Symlink-Schwachstelle				1	2			1	2	2	2	1	1	2			3																1		
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			2	
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	26	12	3

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

5. Labs

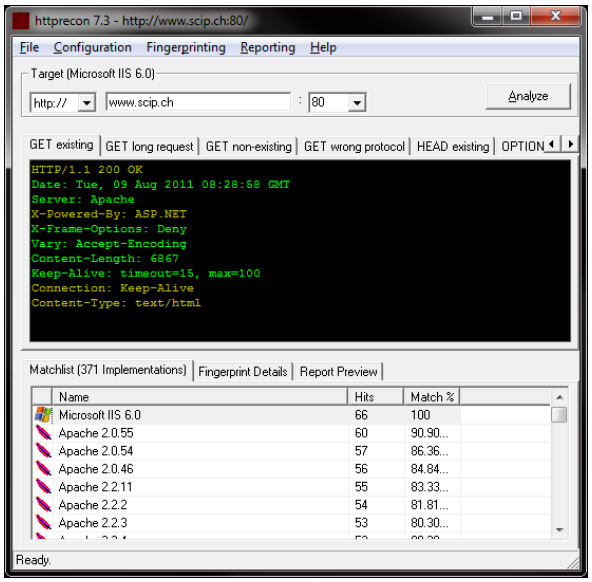
In unseren scip Labs werden unter http://www.scip.ch/?labs regelmässig Neuigkeiten und Forschungsberichte veröffentlicht.

5.1 Einführung in httprecon

18.08.2011 Marc Ruef, maru-at-scip.ch

Das Projekt httprecon wurde im Jahr 2007 gestartet. Hierbei handelt es sich um ein Forschungsprojekt, welches sich mit dem Identifizieren von Webserver-Implementierungen über das Netzwerk auseinandersetzt. Durch das sogenannte *HTTP-Fingerprinting* soll das eingesetzte Produkt identifiziert werden, wodurch zielgerichtete Attacken angestrebt werden können.

Die Windows-Implementierung von httprecon stellt nach dem Aufstarten eine grafische Oberfläche zur Verfügung. Auf dieser kann der Hostname oder die IP-Adresse des Zielsystems definiert werden. Dabei kann zwischen HTTP und HTTPS umgeschaltet und der Zielport ausgewählt werden.



Durch das Drücken des Analyze-Button wird eine Verbindung zum Ziel aufgebaut. Diesem werden verschiedene HTTP-Anfragen geschickt und die Rückantworten ausgewertet. Dabei werden standardmässig die folgenden neun Anfragen genutzt:

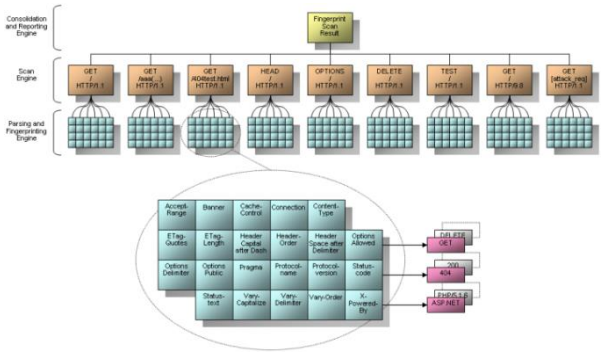
	Anfrage	Beschreibung	Intrusiv
1.	`GET / HTTP/1.1`	Normale GET-Anfrage für existente Ressource	nein
2.	`GET /aaa(...) HTTP/1.1`	Lange GET-Anfrage	ja/nein
3.	`GET /404test.html HTTP/1.1`	GET-Anfrage für nicht-existente Ressource	nein
4.	`HEAD / HTTP/1.1`	Normale HEAD-Anfrage für existierende Ressource	nein
5.	`OPTIONS / HTTP/1.1`	Normale OPTIONS-Anfrage für existierende Ressource	nein
6.	`DELETE / HTTP/1.1`	Normale DELETE-Anfrage für existierende Ressource	ja
7.	`TEST / HTTP/1.1`	HTTP-Anfrage für nicht-existierende Methode	nein
8.	`GET / HTTP/9.8`	HTTP-Anfrage mit nicht-existierender Protokoll-Version	nein
9.	`GET [attack] HTTP/1.1`	GET-Anfrage mit Angriffsstruktur (XSS, SQLi)	ja/nein

Die Antworten werden dann auf verschiedene Merkmale hin untersucht. Dazu gehören in erster Linie:

- Statusinformationen
  - Protokollname
  - Protokollversion
  - Statuscode
  - Statustext
- Header-Werte
  - Accept-Range
  - Banner
  - Cache-Control
  - Connection
  - Content-Type
  - Options-Allowed
  - Options-Public
  - Pragma
  - X-Powered-By
- Header-Struktur
  - Header-Reihenfolge
  - Header Grossschreibung nach Bindestrich
  - Header Leerzeichen nach Aufzählung
  - ETag-Quotes
  - ETag-Länge
  - Options-Trennzeichen
  - Vary-Grossschreibung
  - Vary-Trennzeichen
  - Vary-Reihenfolge

Anhand dieser Merkmale wird quasi ein Fingerabdruck der Webserver-Implementierung erstellt und diese mit der lokalen Fingerabdruck-Datenbank von httprecon verglichen. Dadurch lässt sich derjenige Fingerabdruck mit der

grösstmöglichen Übereinstimmung ausmachen und dadurch das eingesetzte Produkt identifizieren. Die Übereinstimmungen werden in einer Liste samt Details ausgewiesen. Weitere Informationen zur Architektur der Lösungen finden sich auf der Projekt-Webseite.



Durch die erweiterten Konfigurationseinstellungen kann das Verhalten von httprecon den eigenen Bedürfnissen angepasst werden. Zum Beispiel lassen sich die einzelnen Testzugriffe deaktivieren oder deren Attribute verändern (z.B. Zugriff auf welche Ressourcen, Nutzen welcher Methoden). Zusätzlich können neue Webserver-Implementierungen oder Abweichungen bestehender Einträge einfach in die bestehende Datenbank hinzugefügt werden. Dadurch lässt sich die eigene Datenbank beständig erweitern und optimieren. Am Schluss der Analyse können die Resultate in einen Report exportiert und damit im Rahmen einer professionellen Sicherheitsüberprüfung berücksichtigt werden.

6. Impressum

Herausgeber:

)SCIP(
scip ag

scip AG
Badenerstrasse 551
CH-8048 Zürich
T +41 44 404 13 13
info-at-scip.ch
http://www.scip.ch

Zuständige Person:

Marc Ruef
Security Consultant
T +41 44 404 13 13
maru-at-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!