)SCIP(

scip ag

Contents

1. Editorial

Passwörter und ihre Aufbewahrung

Passwörter sind heute ein ganz alltägliches Instrument, anhand deren man auf mehrere Dienste zuzugreifen in der Lage ist. Seien dies Webshops, E-Banking oder Internetforen, alle setzen sie auf irgendeine Art und Weise Passwörter ein, um die Identifikation der Benutzer zu verifizieren.

Passwortsicherheit gilt es aus zwei Sichten zu betrachten: einerseits aus Sicht des Users, andererseits aus Sicht des Dienstanbieters.

Wenn ein User ein Passwort wie 0000, 1234, 123456 oder Password wählt, und dieses Passwort auf möglichst vielen unterschiedlichen Diensten einsetzt, können Dienstanbieter die Passwörter noch so sicher verschlüsselt ablegen, der Schadensfall ist nur noch eine Frage der Zeit.

Abhilfe schafft hier einzig und allein die Sensibilisierung der User. Nur wer korrekt informiert ist, kann eine fundierte Entscheidung treffen. Möchte man die eigenen Gewohnheiten trotzdem nicht ändern, können Passwortmanager oder Browserplugins wie PwdHash dabei helfen, sichere Passwörter zu verwenden, ohne im Komfort eingeschränkt zu werden.

Ein weiterer wichtiger Punkt ist der Einsatz einzigartiger Passwörter pro Webseite. Schliesslich hat ein User keine Macht über die Art und Weise, wie Webseitenbetreiber ihre Benutzerinformationen absichern. Sollte ein Datenklau geschehen, muss man zwangsläufig davon ausgehen, dass das eigene Passwort irgendwann ausfindig gemacht werden wird.

Wenn dasselbe Passwort auf allen vom User benutzten Webseiten eingesetzt wird, haben die Angreifer automatisch Zugriff darauf.

PwdHash umgeht dieses Problem, indem es anhand des eingegebenen Passworts sowie der Webseitendomain einen einzigartigen Hash erzeugt, welcher als Passwort übermittelt wird. Bei Passwortmanagern muss dies erst von Hand geschehen.

Passwortmanager weisen dabei noch ein weiteres Problem auf: die Keychain, in der Passwörter gespeichert werden, ist nur auf dem lokalen Rechner vorhanden. Damit es auf allen Rechnern der User zur Verfügung steht, muss es entweder manuell kopiert oder via Netzwerk/Internet zur Verfügung gestellt werden.

Dies bildet wiederum neue Herausforderungen, die es zu meistern gilt, damit die gewählten Passwörter als sicher zu betrachten sind.

Dienstanbieter andererseits sind in der Pflicht, unabhängig von der Stärke der gewählten Passwörter diese kryptographisch sicher abzulegen.

Dass dies häufig nicht geschieht, wurde in den letzten Wochen verdeutlicht. LinkedIn, eine prominente Social Media Seite, wurde Opfer von gestohlenen Benutzerdaten, gefolgt von vielen weiteren wie Last.fm, eHarmony, Yahoo oder Nvidia.

Die Tatsache, dass die Benutzerdaten gestohlen werden konnten, sagt viel über die Bemühungen aus, die diese Firmen in die Applikationssicherheit (nicht) investiert haben. Hier wären wiederholte Sicherheitsüberprüfungen nötig gewesen, um solche Sicherheitslöcher zu entdecken und zu schliessen.

Aber selbst wenn solche Überprüfungen regelmässig stattgefunden hätten, so ist dennoch zwangsläufig von einem nicht vermeidbaren Restrisiko auszugehen. Daher müssen

Passwörter auf sichere Art und Weise abgelegt werden, um in einem solchen Fall einen letzten Schutz gegen das Auslesen und Bekanntwerden der Passwörter zu haben.

Heutzutage ist klar, dass Passwörter nicht als Plaintext, sondern mittels eines Algorithmus als Hash in der Datenbank gespeichert werden müssen. Als erstes kommt es auf die Wahl des Algorithmus an: MD5 und SHA1 gelten mittlerweile als unsicher und sollten nicht mehr verwendet werden. Zusätzlich gibt es einen zweiten Punkt, der dringend beachtet werden muss: das Salting.

So sind Passwörter, welche ohne sogenanntem Salt gehasht werden, ebenfalls als unsicher zu betrachten. LinkedIn beispielsweise speicherte offenbar sämtliche Passwörter als SHA1-Hash ohne Salt ab, was dazu führte, dass gleich gewählte Passwörter mehrfach in der Datenbank vorhanden waren. Entsprechend musste man diesen Hash nur einmal knacken, um Zugriff auf mehrere Benutzerkonten gleichzeitig zu erhalten.

Wäre ein für jeden User einzigartiger Salt eingesetzt worden, hätte dieses Risiko eliminiert oder schlimmstenfalls drastisch reduziert werden können. Bei der Generierung des Salts sollte unbedingt darauf geachtet werden, dass er nicht zu kurz ist. Eine gute Richtlinie ist der Output des gewählten Algorithmus. SHA256 erzeugt beispielsweise einen Output von 32 Bytes, also sollte das Salt ebenfalls 32 Bytes aufweisen.

Wird ein Passwort auf diese Weise erzeugt, so ist es nun wirklich einzigartig. Sollte der Hash mithilfe des Salts gebrochen werden, sind sämtliche gleich gewählten Passwörter unidentifizierbar, da sie einen anderen Hashwert aufweisen.

Für den Fall, dass ein User eine Passwortänderung vornimmt, muss auch ein neuer Salt generiert werden. Ansonsten läuft man Gefahr, dass eine Passwortänderung nicht viel bringt, sollte einem Angreifer das Salt bekannt sein.

Es gibt also einige Punkte, die es dringend zu **vermeiden** gilt, möchte man Passwörter sicher abspeichern:

- Passwörter als Hash, aber ohne Salt abspeichern
- Ein Passwort einfach doppelt hashen, aber immer noch ohne Salt abspeichern
- Denselben Salt für alle User einsetzen
- Den Usernamen als Salt einsetzen
- Einen zu kurzen Salt einsetzen

Wenn nun die Datenbank trotz aller Bemühungen doch entwendet wird, sind wenigstens die Passwörter einigermassen sicher abgelegt. Dennoch ist es lediglich eine Frage der Zeit, bis sie geknackt werden.

Nun hilft nur noch eine umfassende Informationspolitik. Der Schaden ist bereits angerichtet, Versuche, einen Einbruch zu vertuschen, vergrössern den Schaden meistens.

Eine mögliche erste Reaktion wäre es, sämtliche User per E-Mail zu warnen sowie eine Passwortänderung nahezulegen oder gar zu forcieren und auf der Startseite der betroffenen Webseite eine informationsreiche Warnung aufzuschalten.

Danach muss die ausgenutzte Lücke gefunden und beseitigt werden. Sobald dies getan ist, sollte eine Passwortänderung (erneut) erzwungen werden, damit das gestohlene Passwort nicht verwendet werden kann. Dabei muss sichergestellt werden, dass das gestohlene Passwort nicht erneut gewählt werden kann.

Diese Punkte sind trotz ihrer Ausführlichkeit dennoch nichts weiter als einzelne Aspekte der integralen Sicherheit. Sie zu beachten und umzusetzen ist nicht verkehrt, aber auch nicht als „One Size Fits All“-Lösung zu betrachten.

So individuell wie die einzelnen Webapplikationen sind, so müssen auch die Schutzmassnahmen individuell ausfallen, um eine ganzheitliche Sicherheitslösung zu gewähren.

Schliesslich heisst es nicht umsonst: **„Hoffe stets auf das Beste, aber rechne immer mit dem Schlimmsten“**

Sean Rütschi <seru-at-scip.ch>
Security Consultant
Zürich, 19. Juli 2012

2. scip AG Informationen

2.1 Penetration Test

Das Ziel unserer Dienstleistung Penetration Test ist die Identifikation vorhandener Sicherheitslücken sowie die Definierung der Tragweite dadurch möglicher erfolgreicher Attacken durch Angreifer.

Der Kunde hat ein abgesichertes System vorliegen, das er mittels Ethical Hacking untersucht haben möchte. Um eine wissenschaftliche und wirtschaftliche Optimierung des Auftrags erreichen zu können, wird eine Whitebox-Analyse empfohlen: Der Kunde legt nach Möglichkeiten sämtliche Details zum Zielobjekt offen (IP-Adressen etc.). Somit kann unser Red Team auf eine langwierige Datensammlung verzichten und stattdessen das Expertenwissen auf die Fachgebiete fokussieren.

Das Umsetzen von Penetration Tests basiert zu grossen Teilen auf der systematischen Vorgehensweise, wie sie im Buch „Die Kunst des Penetration Testing“ unseres Herrn Marc Ruef dokumentiert wurde.

- Scanning: Identifizieren von möglichen Angriffsflächen.
- Auswertung: Eingrenzen potentieller Angriffsvektoren, die sich im Rahmen eines konkreten Angriffsszenarios angehen lassen.
- Exploiting: Zielgerichtetes Ausnutzen ausgemachter Sicherheitslücken (Proof-of-Concept).

Ein Penetration Test lässt eine konkrete und verlässliche Aussage bezüglich der existenten Sicherheit eines Systems zu. Die Ausnutzbarkeit von Schwachstellen sowie die Tragweite erfolgreicher Attacken können exakt bestimmt werden, wodurch sich weitere Schritte wie z.B. Risiken akzeptieren oder Gegenmassnahmen einleiten, planen lassen.

Dank unserem ausgewiesenen Expertenwissen kann die scip AG auf eine Vielzahl von Penetration Tests auf unterschiedliche Plattformen, Applikationen und Lösungen zurückblicken.

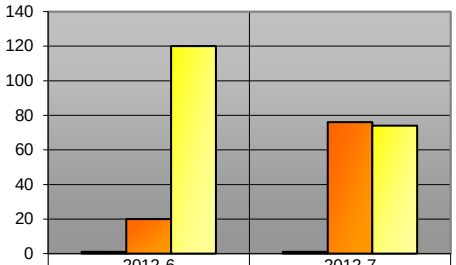
Zählen auch Sie auf uns!
http://www.scip.ch/?firma.referenzenalle

Zögern Sie nicht und kontaktieren Sie unseren Herrn Simon Zumstein unter der Telefonnummer +41 44 404 13 13 oder senden Sie ihm 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



	2012-6	2012-7
sehr kritisch	1	1
kritisch	20	76
problematisch	120	74

Inhalt

2012-2174]
5639 LibTIFF tif_dirread.c TIFFReadDirectory() Pufferüberlauf
5563 VMware Workstation/Fusion/ESX/Player/ESXi Pufferüberlauf
5562 Opera Spoofing [CVE-2012-3558]
5560 Opera Spoofing [CVE-2012-3560]
5558 Opera Small Window Preference Display Pufferüberlauf

3.1 Microsoft Windows win32k.sys Pufferüberlauf [CVE-2012-1890]

Risiko: kritisch
Datum: 10.07.2012
VulDB: http://www.scip.ch/?vuldb.5653

In Microsoft Windows XP/Vista/7/Server 2003/2008, ein Betriebssystem, wurde eine kritische Schwachstelle entdeckt. Davon betroffen ist eine unbekannte Funktion der Datei win32k.sys. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Hiermit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen des Patches MS12-047 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83659) dokumentiert.

3.2 Microsoft Windows win32k.sys Pufferüberlauf [CVE-2012-1893]

Risiko: kritisch
Datum: 10.07.2012
VulDB: http://www.scip.ch/?vuldb.5652

Es wurde eine kritische Schwachstelle in Microsoft Windows XP/Vista/7/Server 2003/2008, ein Betriebssystem, entdeckt. Dies betrifft eine unbekannte Funktion der Datei win32k.sys. Dank der Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dadurch lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen des Patches MS12-047 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83658) dokumentiert.

3.3 Microsoft Data Access Components Pufferüberlauf

Risiko: kritisch
Datum: 10.07.2012
VulDB: http://www.scip.ch/?vuldb.5651

Eine kritische Schwachstelle wurde in Microsoft Data Access Components bis 6.0, ein Betriebssystem, ausgemacht. Betroffen ist eine unbekannte Funktion. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen des Patches MS12-045 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83657) und Secunia (ID 49743) dokumentiert.

3.4 Microsoft Windows Pufferüberlauf [CVE-2012-0175]

Risiko: kritisch
Datum: 10.07.2012
VulDB: http://www.scip.ch/?vuldb.5650

In Microsoft Windows XP/Vista/7/Server 2003/2008, ein Betriebssystem, wurde eine kritische Schwachstelle ausgemacht. Hiervon betroffen ist eine unbekannte Funktion. Mittels dem Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dadurch kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen des Patches MS12-048 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert. Mitunter wird der Fehler

auch in den Datenbanken von OSVDB (ID 83656) und Secunia (ID 49873) dokumentiert.

3.5 Microsoft Office libraries Pufferüberlauf [CVE-2012-1854]

Risiko: kritisch
Datum: 10.07.2012
VulDB: http://www.scip.ch/?vuldb.5649

Es wurde eine kritische Schwachstelle in Microsoft Office bis 2010 SP1 ausgemacht. Davon betroffen ist eine unbekannte Funktion in der Bibliothek libraries. Durch das Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Hiermit kann man Programmcode injizieren. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen des Patches MS12-046 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83655) und Secunia (ID 49800) dokumentiert.

3.6 Microsoft Internet Explorer Pufferüberlauf [CVE-2012-1522]

Risiko: kritisch
Datum: 10.07.2012
VulDB: http://www.scip.ch/?vuldb.5647

In Microsoft Internet Explorer bis 9, ein Webbrowser, wurde eine kritische Schwachstelle gefunden. Betroffen ist eine unbekannte Funktion. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Hiermit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen des Patches MS12-044 lösen. Dieser kann von technet.microsoft.com bezogen werden. Das Problem kann zusätzlich durch den Einsatz von Google Chrome, Mozilla Firefox, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Installieren des jeweiligen Patches empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83653) und Secunia (ID 45690) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.7 Microsoft Internet Explorer Pufferüberlauf [CVE-2012-1524]

Risiko: kritisch
Datum: 10.07.2012
VulDB: http://www.scip.ch/?vuldb.5646

Es wurde eine kritische Schwachstelle in Microsoft Internet Explorer bis 9, ein Webbrowser, gefunden. Hiervon betroffen ist eine unbekannte Funktion. Dank der Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dadurch lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen des Patches MS12-044 beheben. Dieser kann von technet.microsoft.com bezogen werden. Das Problem kann zusätzlich durch den Einsatz von Google Chrome, Mozilla Firefox, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Einspielen des entsprechenden Patches empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Microsoft hat demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83652) und Secunia (ID 45690) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.8 Pidgin libpurple/protocols/mxit/markup.c mxit_show_message() Pufferüberlauf

Risiko: kritisch
Datum: 02.07.2012
VulDB: http://www.scip.ch/?vuldb.5637

Es wurde eine kritische Schwachstelle in Pidgin 2.10.5 gefunden. Davon betroffen ist die Funktion mxit_show_message() der Datei libpurple/protocols/mxit/markup.c. Durch das Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 2.10.5 vermag dieses Problem zu lösen. Das Problem kann auch durch den Einsatz von ICQ/Skype/IRC als alternatives Produkt mitigiert werden. Als

bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Pidgin hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83605) und Secunia (ID 49831) dokumentiert.

3.9 Microsoft Outlook Web App owa/redir.aspx Spoofing

Risiko: kritisch
Datum: 02.07.2012
VulDB: http://www.scip.ch/?vuldb.5636

Eine kritische Schwachstelle wurde in Microsoft Outlook Web App bis 14.1.287.0, ein Mailserver, entdeckt. Dies betrifft eine unbekannte Funktion der Datei owa/redir.aspx. Mittels Manipulieren mit einer unbekannten Eingabe kann eine Spoofing-Schwachstelle ausgenutzt werden. Damit lässt sich Adressfeld vortäuschen. Dies hat Auswirkungen auf die Integrität.

Das Problem kann durch den Einsatz von Zimbra/Hotmail/Gmail als alternatives Produkt mitigiert werden. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83545) dokumentiert.

3.10 Nagios XI Network Monitor SQL Injection

Risiko: kritisch
Datum: 02.07.2012
VulDB: http://www.scip.ch/?vuldb.5633

Eine kritische Schwachstelle wurde in Nagios XI Network Monitor 2011R1.9 ausgemacht. Davon betroffen ist eine unbekannte Funktion. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine SQL Injection-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version CCM Full Beta vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Nagios hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83546) dokumentiert.

3.11 Sun iPlanet Error Page Cross Site Scripting

Risiko: kritisch
Datum: 30.06.2012
VulDB: http://www.scip.ch/?vuldb.5628

Es wurde eine kritische Schwachstelle in Sun iPlanet gefunden. Dies betrifft eine unbekannte Funktion der Komponente Error Page. Dank der Manipulation des Arguments Request URI durch HREF Link kann eine Cross Site Scripting-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit und Integrität.

Die Schwachstelle kann durch das Filtern von Web Server Port mittels Firewalling mitigiert werden. Das Problem kann ebenfalls durch die Einführung von .htaccess als Authentisierung adressiert werden. Das Problem kann weiterhin durch den Einsatz von Apache/MS IIS als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Anwenden von restriktivem Firewalling empfohlen. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83485) dokumentiert.

3.12 Microsoft IIS File Name Tilde Handler erweiterte Rechte

Risiko: kritisch
Datum: 30.06.2012
VulDB: http://www.scip.ch/?vuldb.5623

In Microsoft IIS bis 7.5 wurde eine kritische Schwachstelle ausgemacht. Betroffen ist eine unbekannte Funktion der Komponente File Name Tilde Handler. Durch die Manipulation mit der Eingabe ::$Index_Allocation kann eine erweiterte Rechte-Schwachstelle ausgenutzt werden. Hiermit lässt sich Dateien lesen. Dies hat Auswirkungen auf Vertraulichkeit und Integrität.

Die Schwachstelle kann durch das Filtern von Web Server Port mittels Firewalling mitigiert werden. Das Problem kann ebenfalls durch den Einsatz von Apache als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von SecurityFocus (ID 54251) dokumentiert.

3.13 Avaya IP Office Customer Call Reporter ImageUpload.ashx erweiterte Rechte

Risiko: kritisch
Datum: 28.06.2012
VulDB: http://www.scip.ch/?vuldb.5632

In Avaya IP Office Customer Call Reporter 7.x/8.x wurde eine kritische Schwachstelle ausgemacht. Dies betrifft eine unbekannte Funktion der Datei ImageUpload.ashx. Mittels

dem Manipulieren durch PHP File kann eine erweiterte Rechte-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit und Integrität.

Ein Upgrade auf die Version 7.0.5.8/8.0.9.13 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Avaya hat demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83399) und Secunia (ID 49762) dokumentiert.

3.14 SAP NetWeaver msg_server.exe Pufferüberlauf

Risiko: kritisch
Datum: 28.06.2012
VulDB: http://www.scip.ch/?vuldb.5630

Eine kritische Schwachstelle wurde in SAP NetWeaver gefunden. Hiervon betroffen ist eine unbekannte Funktion der Komponente msg&#095server.exe. Mittels Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als bestmögliche Massnahme wird das Einspielen des entsprechenden Patches empfohlen. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83494) und Secunia (ID 49744) dokumentiert.

3.15 Cisco WebEx Recording Format Player Pufferüberlauf

Risiko: kritisch
Datum: 27.06.2012
VulDB: http://www.scip.ch/?vuldb.5627

Eine kritische Schwachstelle wurde in Cisco WebEx Recording Format Player bis 28.0.0 (T28 L10N) entdeckt. Betroffen ist eine unbekannte Funktion. Durch das Beeinflussen durch Datei kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 28.1.0 (T28 L10N SP1) vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83352) und Secunia (ID 49750) dokumentiert.

3.16 Cisco WebEx Recording Format Player Pufferüberlauf

Risiko: kritisch
Datum: 27.06.2012
VulDB: http://www.scip.ch/?vuldb.5626

In Cisco WebEx Recording Format Player bis 28.0.0 (T28 L10N) wurde eine kritische Schwachstelle entdeckt. Hiervon betroffen ist eine unbekannte Funktion. Mittels dem Manipulieren durch Datei kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dadurch kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 28.1.0 (T28 L10N SP1) vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83351) und Secunia (ID 49750) dokumentiert.

3.17 Cisco WebEx Recording Format Player Pufferüberlauf

Risiko: kritisch
Datum: 27.06.2012
VulDB: http://www.scip.ch/?vuldb.5625

Es wurde eine kritische Schwachstelle in Cisco WebEx Recording Format Player bis 28.0.0 (T28 L10N) entdeckt. Davon betroffen ist eine unbekannte Funktion. Durch das Manipulieren durch Datei kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Hiermit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 28.1.0 (T28 L10N SP1) vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83350) und Secunia (ID 49750) dokumentiert.

3.18 Cisco WebEx Recording Format Player Pufferüberlauf

Risiko: kritisch
Datum: 27.06.2012
VulDB: http://www.scip.ch/?vuldb.5624

Eine kritische Schwachstelle wurde in Cisco WebEx Recording Format Player bis 28.0.0 (T28 L10N) ausgemacht. Dies betrifft eine unbekannte Funktion. Mittels Manipulieren durch Datei kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 28.1.0 (T28 L10N SP1) vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83349) und Secunia (ID 49750) dokumentiert.

3.19 Google Chrome XML libxml Pufferüberlauf [CVE-2012-2807]

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5611

In Google Chrome bis 19.0.1084.57 (Linux 64-bit), ein Webbrowser, wurde eine kritische Schwachstelle gefunden. Betroffen ist eine unbekannte Funktion in der Bibliothek libxml der Komponente XML. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 20.0.1132.43 vermag dieses Problem zu lösen. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83266) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.20 Google Chrome Matroska Container Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5609

Eine kritische Schwachstelle wurde in Google Chrome bis 19.0.1084.57, ein Webbrowser, entdeckt. Davon betroffen ist eine unbekannte Funktion der Komponente Matroska Container. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 20.0.1132.43 vermag dieses Problem zu lösen. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83250) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.21 Google Chrome PDF JS API Pufferüberlauf [CVE-2012-2833]

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5608

In Google Chrome bis 19.0.1084.57, ein Webbrowser, wurde eine kritische Schwachstelle entdeckt. Dies betrifft eine unbekannte Funktion der Komponente PDF JS API. Mittels dem Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 20.0.1132.43 vermag dieses Problem zu beheben. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort

reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83249) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.22 Google Chrome SVG Reference Handler Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5606

Eine kritische Schwachstelle wurde in Google Chrome bis 19.0.1084.57, ein Webbrowser, ausgemacht. Hiervon betroffen ist eine unbekannte Funktion der Komponente SVG Reference Handler. Mittels Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 20.0.1132.43 vermag dieses Problem zu beheben. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83257) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.23 Google Chrome First-Letter Handler Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5603

Eine kritische Schwachstelle wurde in Google Chrome bis 19.0.1084.57, ein Webbrowser, gefunden. Betroffen ist eine unbekannte Funktion der Komponente First-Letter Handler. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 20.0.1132.43 vermag dieses Problem zu lösen. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83256) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.24 Google Chrome PDF Pufferüberlauf [CVE-2012-2828]

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5602

In Google Chrome bis 19.0.1084.57, ein Webbrowser, wurde eine kritische Schwachstelle gefunden. Hiervon betroffen ist eine unbekannte Funktion der Komponente PDF. Mittels dem Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 20.0.1132.43 vermag dieses Problem zu beheben. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83240) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.25 Google Chrome User Interface Pufferüberlauf [CVE-2012-2827]

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5601

Es wurde eine kritische Schwachstelle in Google Chrome bis 19.0.1084.57 (Mac), ein Webbrowser, gefunden. Davon betroffen ist eine unbekannte Funktion der Komponente User Interface. Durch das Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 20.0.1132.43 vermag dieses Problem zu lösen. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83239) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.26 Google Chrome Texture Conversion Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5600

Eine kritische Schwachstelle wurde in Google Chrome bis 19.0.1084.57, ein Webbrowser, entdeckt. Dies betrifft eine unbekannte Funktion der Komponente Texture Conversion. Mittels Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 20.0.1132.43 vermag dieses Problem zu beheben. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83247) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.27 Google Chrome SVG Painting Handler Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5599

In Google Chrome bis 19.0.1084.57, ein Webbrowser, wurde eine kritische Schwachstelle entdeckt. Betroffen ist eine unbekannte Funktion der Komponente SVG Painting Handler. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 20.0.1132.43 vermag dieses Problem zu lösen. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83246) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.28 Google Chrome SVG Resource Handler Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5598

Es wurde eine kritische Schwachstelle in Google Chrome bis 19.0.1084.57, ein Webbrowser, entdeckt. Hiervon betroffen ist eine unbekannte Funktion der Komponente SVG Resource Handler. Dank der Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 20.0.1132.43 vermag dieses Problem zu beheben. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83245) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.29 Google Chrome Counter Layout Handler Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5588

Eine kritische Schwachstelle wurde in Google Chrome bis 19.0.1084.57, ein Webbrowser, ausgemacht. Dies betrifft eine unbekannte Funktion der Komponente Counter Layout Handler. Mittels Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 20.0.1132.43 vermag dieses Problem zu beheben. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83242) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.30 Google Chrome Table Selection Handler Pufferüberlauf

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5587

In Google Chrome bis 19.0.1084.57, ein Webbrowser, wurde eine kritische Schwachstelle ausgemacht. Betroffen ist eine unbekannte Funktion der Komponente Table Selection Handler. Durch die Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 20.0.1132.43 vermag dieses Problem zu lösen. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Upgrade auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83238) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.31 Google Chrome Sandbox erweiterte Rechte [CVE-2012-2816]

Risiko: kritisch
Datum: 26.06.2012
VulDB: http://www.scip.ch/?vuldb.5586

Es wurde eine kritische Schwachstelle in Google Chrome bis 19.0.1084.57 (Windows), ein Webbrowser, ausgemacht. Hiervon betroffen ist eine unbekannte Funktion der Komponente Sandbox. Dank der Manipulation mit einer unbekannten Eingabe kann eine erweiterte Rechte-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 20.0.1132.43 vermag dieses Problem zu beheben. Eine neue Version kann von google.com bezogen werden. Das Problem kann auch durch den Einsatz von Mozilla Firefox, Microsoft Internet Explorer, Opera als alternatives Produkt mitigiert werden. Als bestmögliche Massnahme wird das Aktualisieren auf eine neue Version empfohlen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Google hat demnach sofort reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83253) dokumentiert. In deutscher Sprache berichtet unter anderem Heise zum Fall.

3.32 Red Hat Red Hat Package Manager erweiterte Rechte

Risiko: kritisch
Datum: 25.06.2012
VulDB: http://www.scip.ch/?vuldb.5596

In Red Hat Red Hat Package Manager bis 4.8.0 wurde eine kritische Schwachstelle ausgemacht. Dies betrifft eine unbekannte Funktion. Mittels dem Manipulieren mit einer unbekannten Eingabe kann eine erweiterte Rechte-Schwachstelle ausgenutzt werden. Dadurch kann man Home Directory löschen. Dies hat Auswirkungen auf Vertraulichkeit und Integrität.

Ein Upgrade auf die Version 4.9.1.3 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Red Hat

hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83222) und Secunia (ID 49680) dokumentiert.

3.33 Red Hat RPM Package Manager fsm.c erweiterte Rechte

Risiko: kritisch
Datum: 24.06.2012
VulDB: http://www.scip.ch/?vuldb.5619

Es wurde eine kritische Schwachstelle in Red Hat RPM Package Manager bis 4.9.1.2 gefunden. Betroffen ist eine unbekannte Funktion der Datei fsm.c. Durch das Manipulieren mit einer unbekannten Eingabe kann eine erweiterte Rechte-Schwachstelle ausgenutzt werden. Hiermit kann man einfach erweiterte Zugriffe durchführen. Dies hat Auswirkungen auf Vertraulichkeit und Integrität.

Ein Aktualisieren auf die Version 4.9.1.3 vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Red Hat hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83269) und Secunia (ID 49680) dokumentiert.

3.34 Debian dhcpcd DHCP Client Pufferüberlauf [CVE-2012-2152]

Risiko: kritisch
Datum: 23.06.2012
VulDB: http://www.scip.ch/?vuldb.5597

Eine kritische Schwachstelle wurde in Debian dhcpcd bis 3.2.3 (Linux), ein Betriebssystem, ausgemacht. Davon betroffen ist eine unbekannte Funktion der Komponente DHCP Client. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 4.0.2 vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Debian hat demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83228) und Secunia (ID 49679) dokumentiert.

3.35 NullSoft WinAmp in_mod.dll Pufferüberlauf

Risiko: kritisch
Datum: 20.06.2012
VulDB: http://www.scip.ch/?vuldb.5615

Eine kritische Schwachstelle wurde in NullSoft WinAmp bis 5.63, ein Multimediaplayer, ausgemacht. Betroffen ist eine unbekannte Funktion in der Bibliothek _in_mod.dll_. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 5.63 Build 3234 vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. NullSoft hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83098) dokumentiert.

3.36 NullSoft WinAmp in_avi.dll Pufferüberlauf

Risiko: kritisch
Datum: 20.06.2012
VulDB: http://www.scip.ch/?vuldb.5614

In NullSoft WinAmp bis 5.63, ein Multimediaplayer, wurde eine kritische Schwachstelle ausgemacht. Hiervon betroffen ist eine unbekannte Funktion in der Bibliothek _in_avi.dll_. Mittels dem Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 5.63 Build 3234 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. NullSoft hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83098) dokumentiert.

3.37 NullSoft WinAmp TSCC Decoder Pufferüberlauf

Risiko: kritisch
Datum: 20.06.2012
VulDB: http://www.scip.ch/?vuldb.5613

Es wurde eine kritische Schwachstelle in NullSoft WinAmp bis 5.63, ein Multimediaplayer, ausgemacht. Davon betroffen ist eine unbekannte Funktion der Komponente TSCC Decoder. Durch das Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 5.63 Build 3234 vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. NullSoft hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83098) dokumentiert.

3.38 Apple iTunes Pufferüberlauf

Risiko: kritisch
Datum: 20.06.2012
VulDB: http://www.scip.ch/?vuldb.5594

Eine kritische Schwachstelle wurde in Apple iTunes bis 10.6.1.7 gefunden. Hiervon betroffen ist eine unbekannte Funktion. Mittels Manipulieren durch Datei kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als bestmögliche Massnahme wird das Einspielen des entsprechenden Patches empfohlen. Das Erscheinen einer Gegenmassnahme geschah schon vor und nicht nach der Veröffentlichung der Schwachstelle. Apple hat demnach vorab reagiert. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83220) dokumentiert.

3.39 NullSoft WinAmp in_mod.dll Pufferüberlauf

Risiko: kritisch
Datum: 20.06.2012
VulDB: http://www.scip.ch/?vuldb.5579

Eine kritische Schwachstelle wurde in NullSoft WinAmp bis 5.63, ein Multimediaplayer, ausgemacht. Betroffen ist eine unbekannte Funktion in der Bibliothek _in_mod.dll_. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 5.63 Build 3234 vermag dieses Problem zu lösen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. NullSoft hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83098) und Secunia (ID 46624) dokumentiert.

3.40 NullSoft WinAmp bmp.w5s Pufferüberlauf

Risiko: kritisch
Datum: 20.06.2012
VulDB: http://www.scip.ch/?vuldb.5578

In NullSoft WinAmp 5.622, ein Multimediaplayer, wurde eine kritische Schwachstelle ausgemacht. Hiervon betroffen ist eine unbekannte Funktion der Komponente bmp.w5s. Mittels dem Manipulieren durch AVI File kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 5.63 Build 3234 vermag dieses Problem zu beheben. Eine neue Version kann von forums.winamp.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. NullSoft hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83097) und Secunia (ID 46624) dokumentiert.

3.41 Cisco AnyConnect Secure Mobility Client VPN Downloader WebLaunch Pufferüberlauf

Risiko: kritisch
Datum: 20.06.2012
VulDB: http://www.scip.ch/?vuldb.5577

Es wurde eine kritische Schwachstelle in Cisco AnyConnect Secure Mobility Client bis 3.0 ausgemacht. Davon betroffen ist die Funktion WebLaunch der Komponente VPN Downloader. Durch das Manipulieren durch Java/ActiveX kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Hiermit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren vermag dieses Problem zu lösen. Eine neue Version kann von tools.cisco.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. Cisco hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83096), Secunia (ID 49645) und SecurityFocus (ID 54107) dokumentiert.

3.42 Linux Kernel KVM Subsystem setup_routing_entry() Pufferüberlauf

Risiko: kritisch
Datum: 19.06.2012
VulDB: http://www.scip.ch/?vuldb.5582

Eine kritische Schwachstelle wurde in Linux Kernel, ein Betriebssystem, entdeckt. Hiervon betroffen ist die Funktion setup_routing_entry() der Komponente KVM Subsystem. Mittels Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade vermag dieses Problem zu beheben. Eine neue Version kann von rhn.redhat.com bezogen werden. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83104) und Secunia (ID 49625) dokumentiert.

3.43 Ffmpeg Pufferüberlauf [CVE-2012-0859]

Risiko: kritisch
Datum: 19.06.2012
VulDB: http://www.scip.ch/?vuldb.5570

Eine kritische Schwachstelle wurde in Ffmpeg bis 0.9.3 ausgemacht. Hiervon betroffen ist eine unbekannte Funktion. Mittels Manipulieren mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Die Schwachstelle lässt sich durch das Einspielen eines Patches beheben. Dieser kann von gitorious.org bezogen werden. Das Erscheinen einer Gegenmassnahme geschah vor und nicht erst nach der Veröffentlichung der Schwachstelle. Die Entwickler haben demnach vorgängig reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83055) und Secunia (ID 49621) dokumentiert.

3.44 Mozilla Firefox nsHTMLSelectElement.cpp nsHTMLSelectElement Pufferüberlauf

Risiko: kritisch
Datum: 18.06.2012
VulDB: http://www.scip.ch/?vuldb.5574

Es wurde eine kritische Schwachstelle in Mozilla Firefox bis 8.0, ein Webbrowser, gefunden. Hiervon betroffen ist die Funktion nsHTMLSelectElement der Datei nsHTMLSelectElement.cpp. Dank der Manipulation mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 9.0 vermag dieses Problem zu beheben. Mitunter wird der Fehler auch in der Verwundbarkeitsdatenbank von OSVDB (ID 83115) dokumentiert.

3.45 IBM Lotus Notes Pufferüberlauf [CVE-2012-2174]

Risiko: kritisch
Datum: 18.06.2012
VulDB: http://www.scip.ch/?vuldb.5573

Eine kritische Schwachstelle wurde in IBM Lotus Notes bis 8.5.3 entdeckt. Davon betroffen ist eine unbekannte Funktion. Durch das Beeinflussen mit einer unbekannten Eingabe kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Als bestmögliche Massnahme wird das Installieren des jeweiligen Patches empfohlen. Das Erscheinen einer Gegenmassnahme geschah sofort nach der Veröffentlichung der Schwachstelle. IBM hat demnach unmittelbar reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83063) und Secunia (ID 49601) dokumentiert.

3.46 LibTIFF tif_dirread.c TIFFReadDirectory() Pufferüberlauf

Risiko: kritisch
Datum: 15.06.2012
VulDB: http://www.scip.ch/?vuldb.5639

Eine kritische Schwachstelle wurde in LibTIFF bis 3.9.4 gefunden. Betroffen ist die Funktion TIFFReadDirectory() der Datei _tif_dirread.c_. Durch das Beeinflussen durch Datei kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Damit kann man Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren auf die Version 4.0.2 vermag dieses Problem zu lösen. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 83628) und Secunia (ID 49833) dokumentiert.

3.47 VMware Workstation/Fusion/ESX/Player/ESXi Pufferüberlauf

Risiko: kritisch
Datum: 14.06.2012
VulDB: http://www.scip.ch/?vuldb.5563

In VMware Workstation/Fusion/ESX/Player/ESXi, ein Virtualisierungslösung, wurde eine kritische Schwachstelle entdeckt. Betroffen ist eine unbekannte Funktion. Durch die Manipulation durch Datei kann eine Pufferüberlauf-Schwachstelle ausgenutzt werden. Hiermit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Aktualisieren vermag dieses Problem zu lösen. Eine neue Version kann von vmware.com bezogen werden. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. VMware hat demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 82979), Secunia (ID 49430) und SecurityFocus (ID 53996) dokumentiert.

3.48 Opera Spoofing [CVE-2012-3558]

Risiko: kritisch
Datum: 14.06.2012
VulDB: http://www.scip.ch/?vuldb.5562

Es wurde eine kritische Schwachstelle in Opera bis 12.00 Beta, ein Webbrowser, entdeckt. Hiervon betroffen ist eine unbekannte Funktion. Dank der Manipulation mit einer unbekannten Eingabe kann eine Spoofing-Schwachstelle ausgenutzt werden. Dadurch lässt sich Adressfeld vortäuschen. Dies hat Auswirkungen auf die Integrität.

Ein Upgrade auf die Version 12.00 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Die Entwickler haben demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 82955) und Secunia (ID 49533) dokumentiert.

3.49 Opera Spoofing [CVE-2012-3560]

Risiko: kritisch
Datum: 14.06.2012
VulDB: http://www.scip.ch/?vuldb.5560

In Opera bis 12.00 Beta, ein Webbrowser, wurde eine kritische Schwachstelle ausgemacht. Dies betrifft eine unbekannte Funktion. Mittels dem Manipulieren mit einer unbekannten Eingabe kann eine Spoofing-Schwachstelle ausgenutzt werden. Dadurch kann man Adressfeld vortäuschen. Dies hat Auswirkungen auf die Integrität.

Ein Upgrade auf die Version 12.00 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Die Entwickler haben demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 82953) und Secunia (ID 49533) dokumentiert.

3.50 Opera Small Window Preference Display Pufferüberlauf

Risiko: kritisch
Datum: 14.06.2012
VulDB: http://www.scip.ch/?vuldb.5558

Eine kritische Schwachstelle wurde in Opera bis 12.00 Beta, gefunden. Hiervon betroffen ist eine Funktion der Komponente Small Window Preference Display. Mittels Eingabemanipulation kann ein Pufferüberlauferzeugt werden. Damit lässt sich Programmcode ausführen. Dies hat Auswirkungen auf Vertraulichkeit, Integrität und Verfügbarkeit.

Ein Upgrade auf die Version 12.00 vermag dieses Problem zu beheben. Das Erscheinen einer Gegenmassnahme geschah direkt nach der Veröffentlichung der Schwachstelle. Die Entwickler haben demnach sofort reagiert. Mitunter wird der Fehler auch in den Datenbanken von OSVDB (ID 82951) und Secunia (ID 49533) dokumentiert.

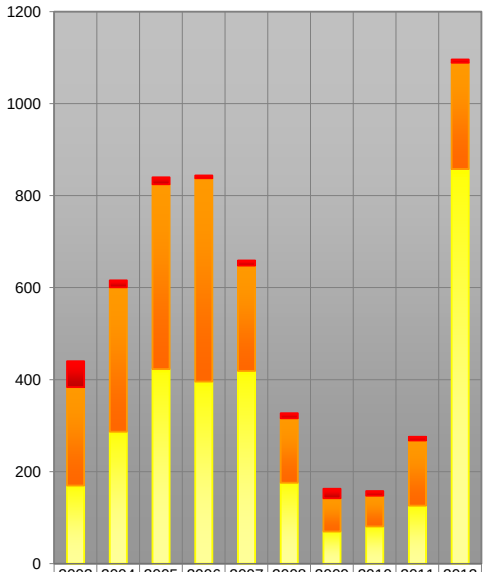
4. Statistiken Verletzbarkeiten

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

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

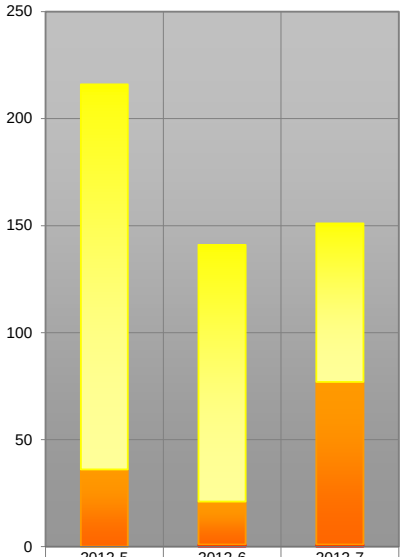
Zögern Sie nicht uns zu kontaktieren. Falls Sie spezifische Statistiken aus unserer Verletzbarkeitsdatenbank wünschen so senden Sie uns eine E-Mail an info-at-scip.ch. Gerne nehmen wir Ihre Vorschläge entgegen.

Auswertungsdatum:	18. Juli 2012



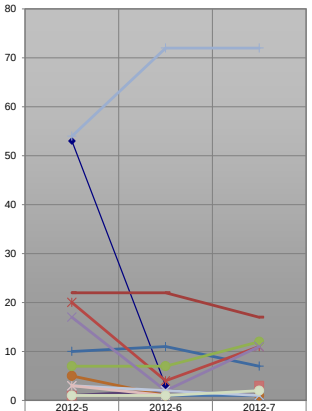
	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012
sehr kritisch	56	15	15	6	11	11	21	10	8	7
kritisch	214	314	402	442	229	140	72	67	142	231
problematisch	170	287	423	396	419	176	70	81	126	858

Verlauf der Anzahl Schwachstellen pro Jahr



	2012-5	2012-6	2012-7
problematisch	180	120	74
kritisch	36	20	76
sehr kritisch		1	1

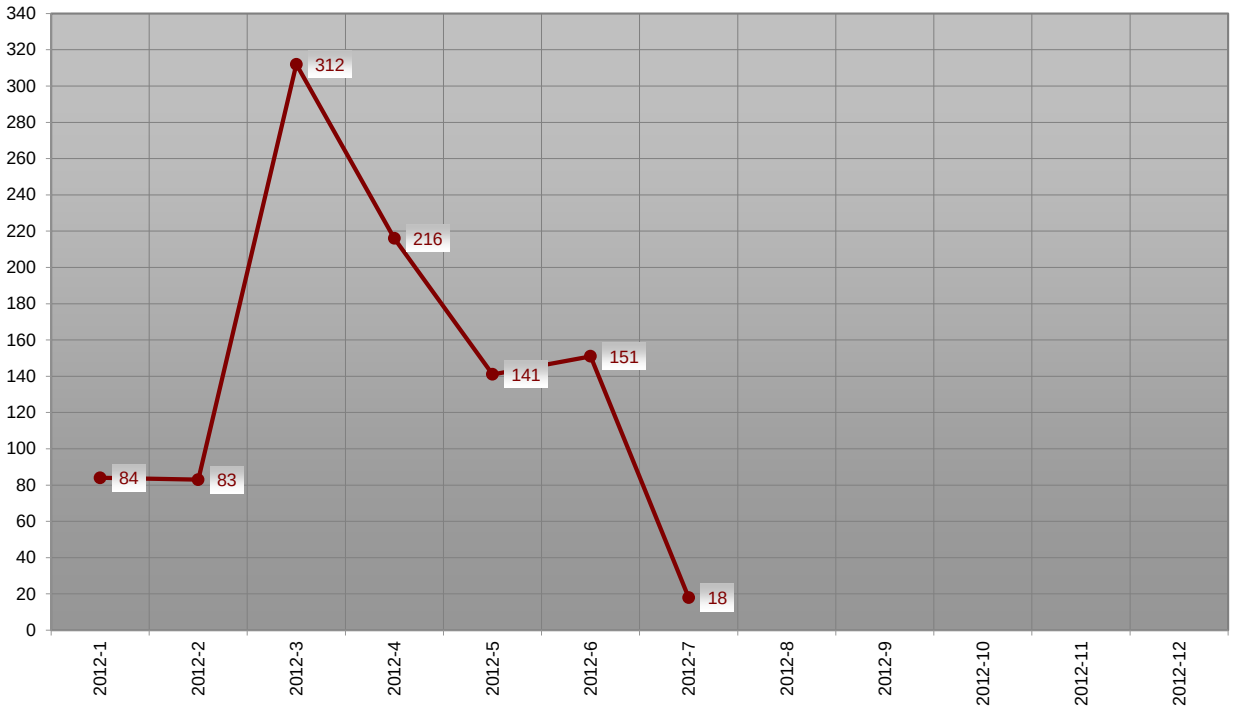
Verlauf der letzten drei Monate Schwachstelle/Schweregrad



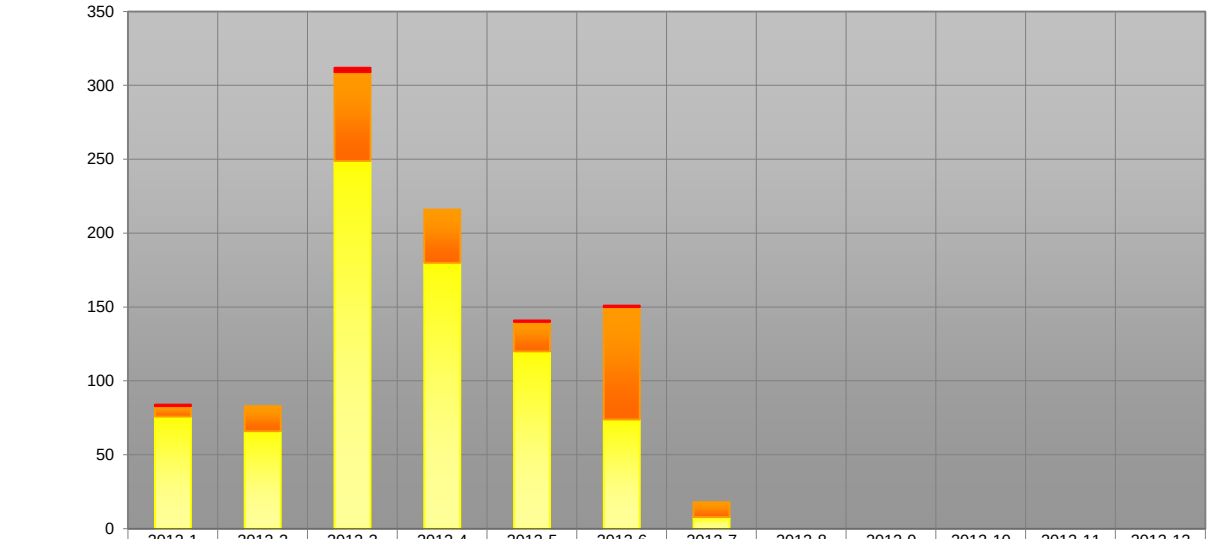
	2012-5	2012-6	2012-7
Unbekannt	53	3	
Authentisierung umgehen			
Code Injection			
Command Injection	1	2	1
Cross Site Redirect		1	
Cross Site Request Forgery	5	1	1
Cross Site Scripting	10	11	7
Denial of Service	22	22	17
Designfehler			
Directory Traversal			2
Eingabeungültigkeit			
erweiterte Dateirechte			
erweiterte Leserechte		1	1
erweiterte Rechte	20	4	11
erweiterte Zugriffsrechte	7	7	12
Fehlende Authentifizierung			
Fehlende Verschlüsselung			
Fehlerhafte Leserechte			
Fehlerhafte Schreibrechte			
Fehlkonfiguration	1		3
Format String			
Information Disclosure	17	2	11
Konfigurationsfehler			
Programmcode ausführen			
Pufferüberlauf	54	72	72
Race Condition	1	1	
Race-Condition			
Redirect			
Remote File Inclusion			
Schwache Authentifizierung			
schwache Authentisierung	3	2	1
Schwache Verschlüsselung	3	1	
Spoofing	1	1	2

Verlauf der letzten drei Monate Schwachstelle/Kategorie

Registrierte Schwachstellen by scip AG

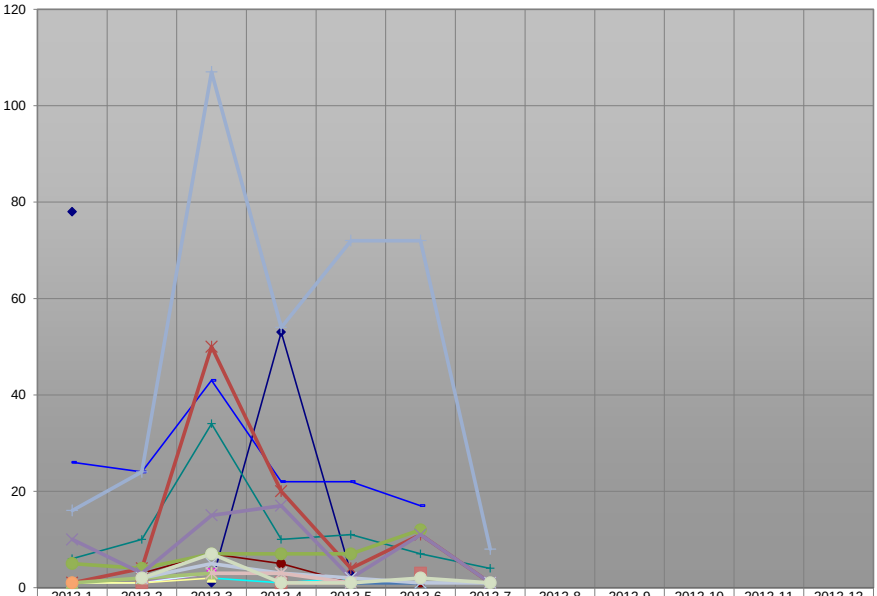


Verlauf der Anzahl Schwachstellen pro Monat - Zeitperiode 2012



	2012-1	2012-2	2012-3	2012-4	2012-5	2012-6	2012-7	2012-8	2012-9	2012-10	2012-11	2012-12
sehr kritisch	1		3		1	1						
kritisch	7	17	60	36	20	76	10					
problematisch	76	66	249	180	120	74	8					

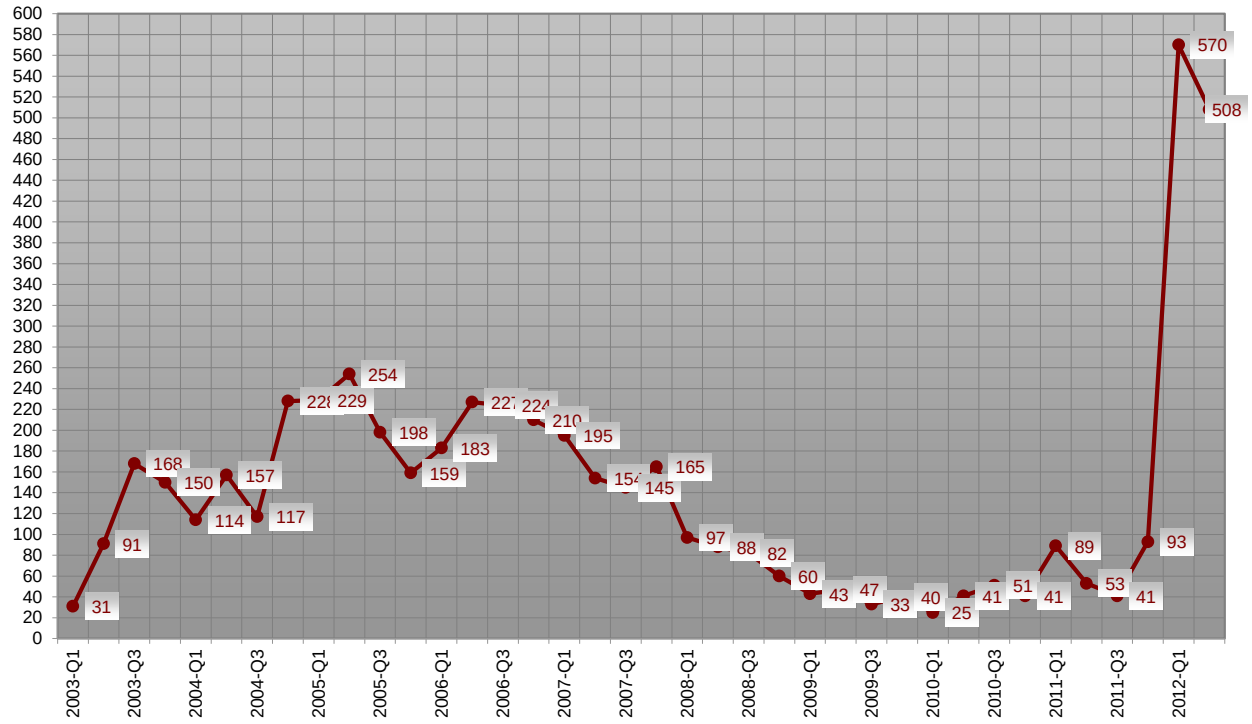
Verlauf der Anzahl Schwachstellen/Schweregrad pro Monat - Zeitperiode 2012



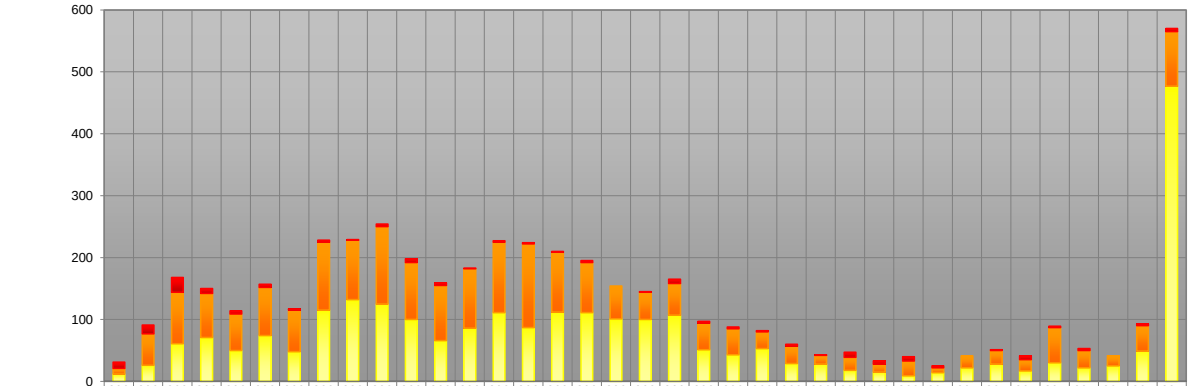
	2012-1	2012-2	2012-3	2012-4	2012-5	2012-6	2012-7	2012-8	2012-9	2012-10	2012-11	2012-12
Unbekannt	78		1	53	3							
Authentisierung umgehen		1	3									
Code Injection	1											
Command Injection	5		2	1	2	1						
Cross Site Redirect					1							
Cross Site Request Forgery		3	7	5	1	1	1					
Cross Site Scripting	6	10	34	10	11	7	4					
Denial of Service	26	24	43	22	22	17						
Designfehler												
Directory Traversal	1	1	3			2						
Eingabeungültigkeit												
erweiterte Dateirechte	1	1	2									
erweiterte Leserechte		1			1	1						
erweiterte Rechte	1	4	50	20	4	11	1					
erweiterte Zugriffsrechte	5	4	7	7	7	12						
Fehlende Authentifizierung												
Fehlende Verschlüsselung												
Fehlerhafte Leserechte												
Fehlerhafte Schreibrechte												
Fehlkonfiguration		1		1		3						
Format String	1	2	3									
Information Disclosure	10	3	15	17	2	11	1					
Konfigurationsfehler												
Programmcode ausführen	1											
Pufferüberlauf	16	24	107	54	72	72	8					
Race Condition		1		1	1							
Race-Condition												
Redirect												
Remote File Inclusion												
Schwache Authentifizierung												
schwache Authentisierung		2	5	3	2	1	1					
Schwache Verschlüsselung			3	3	1							
Spoofing		2	7	1	1	2	1					

Verlauf der Anzahl Schwachstellen/Kategorie pro Monat - Zeitperiode 2012

Registrierte Schwachstellen by scip AG

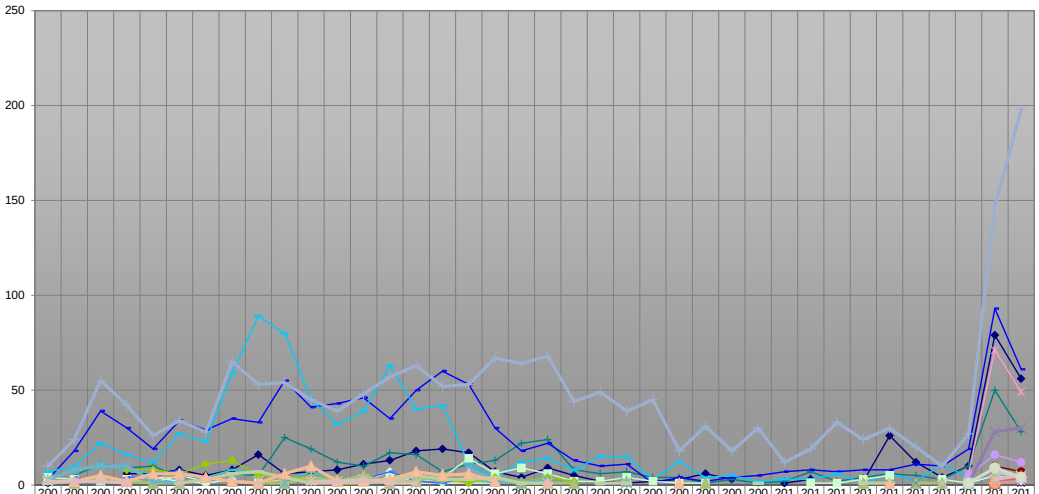


Verlauf der Anzahl Schwachstellen pro Quartal seit Q1/2003



	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	2011-Q4	2012-Q1
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		3	5
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	41	88
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	25	49	477

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	2011-Q4	2012-Q1	2012-Q2
Unbekannt	1			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	4	10	79	56
Authentisierung umgehen																			1																	4	
Code Injection																																				1	
Command Injection																																				7	4
Cross Site Redirect																																					1
Cross Site Request Forgery																																				10	7
Cross Site Scripting		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	4	6	5	3	10	50	28
Denial of Service	3	18	39	30	19	34	29	35	33	55	41	43	46	35	50	60	53	30	18	22	13	10	11	1	4	2	4	5	7	8	7	8	8	11	10	19	93	61
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	11	4		
Directory Traversal					4	2	1	3		4	2	3	2	7	1	1	1	1													1		1			1	5	2
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	1		
erweiterte Dateirechte																																				4	
erweiterte Leserechte																																				1	2
erweiterte Rechte																										1						1				6	71	49
erweiterte Zugriffsrechte																																				5	16	12
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		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				
Fehlkonfiguration																																				1	4
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	1		6	
Information Disclosure																																		1		1	28	30
Konfigurationsfehler	3	8	10	10	2	1		3		1							9	2	1	3			1															
Programmcode ausführen																																				1	
Pufferüberlauf	10	24	55	42	26	34	28	65	53	54	45	39	48	57	63	52	53	67	64	68	44	49	39	45	18	31	18	30	12	19	33	24	30	20	10	27	147	198
Race Condition																																					1	2
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				
Redirect																																				1		
Remote File Inclusion																																				1		
Schwache Authentifizierung		2	5	2	6	6	4	2	1	6	10	2	2	3	7	5	6	2		1					1								1				
schwache Authentisierung																																			1		7	4
Schwache Verschlüsselung	2	2	2	1		1			2		2	2	3	1	1					1																3	5
Spoofing																																				1	9	4

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 Information statt Angst

12.07.2012 Stefan Friedli, stfr-at-scip.ch

IT-Sicherheit beschäftigt. In unserem Alltag werden wir zunehmend mit dem Schutz unserer eigenen Daten und Privatsphäre konfrontiert. Firmeninhaber sehen sich durch Industriespionage und dem Ausfall von Systemen durch Virenbefall bedroht. Politiker zucken zusammen, wenn der Kunstbegriff “Cyberterrorismus” die Runde macht.

Technologie ist ein komplexes Thema. Im Alltag unserer Gesellschaft erhöht sich diese Komplexität noch einmal massiv, weil Technologie sich mit politischen, wirtschaftlichen, ethischen und moralischen Faktoren untrennbar verkettet. Reden wir dann von der Sicherheit dieser Technologien, so reden wir auch vom Einfluss auf alle damit verwobenen gesellschaftlichen Verknüpfungen.

Virenangriffe wie Stuxnet sind ein exzellentes Beispiel: Natürlich ist der Angriffsmechanismus interessant. Ebenso die Schwachstellen, die ausgenutzt wurden. Doch was Stuxnet zu einem Thema der Massen machte, ist der Fakt, dass (angeblich) Atomkraftwerke angegriffen werden sollte. Dass Vermutungen im Raum stehen, dass es sich hier um digitale Kriegsführung handelt, einem realen Konflikt zwischen realen Staaten – mit den komplexen technologischen Grundlagen hat das aber nichts mehr zu tun.

Es ist heute weitgehend bekannt, dass Technologie Schwachstellen aufweist. Die Existenz von Hackern ist, so sehr sie auch sensationalisiert und verfälscht dargestellt wird, eine unumstrittene Tatsache. Einige Themen und Begriffe, wie zum Beispiel Computerviren und Trojaner sind dermassen oft schon in der Öffentlichkeit aufgetaucht, dass sie Common Knowledge sind. Die Mainstream Medien arbeiten mit diesen Begriffen und, oftmals selbsternannte, “Experten” nutzen dieselbe Terminologie, um ihre Kredibilität zu unterstreichen und sich gegenüber den Medien und der Öffentlichkeit verständlich zu machen. IT-Sicherheit ist ein Thema, über das gesprochen wird.

Wir sprechen über Virenattacken, über Keylogger und Trojaner und wie wir uns davor schützen können. Das ist gut, aber es gibt eine schlechte Nachricht: Wir sprechen über 2% des Problems – und das ist eine optimistische Schätzung. Die restlichen 98% des Problems werden nicht angesprochen, weil sie nach dem Ermessen irgendwelcher Leute in eine der folgenden Kategorien fallen:

1. Der Inhalt ist technisch zu komplex für die breite Masse
2. Das Szenario des Problems ist für einen grossen Teil der Masse nicht nachvollziehbar
3. Niemand hat bislang eine Möglichkeit gefunden, damit Geld zu verdienen

Alle drei Kategorien sind kurzsichtig, unlogisch sowie, abhängig vom jeweiligen Fall aus journalistischem Blickwinkel falsch und unmoralisch.

Die wenigen Themen, die wir effektiv ansprechen, sind meistens trivial und veraltet. Wir erhalten zum Beispiel regelmässig Presseanfragen zum Thema Computerviren – erst vor kurzem wurde ich in einem Radiointerview nach Dingen gefragt, die seit 10 Jahren in Hunderten von Artikel geschrieben wurden: Was ist ein Virus? Kann man sich schützen? Wie gut sind AV Produkte?

Sind diese Fragen legitim? Ja. Gäbe es bessere Fragen: Definitiv.

Vor kurzem wurde ich von einem Journalisten gefragt, was ich von der Berichterstattung in unserem Sektor halte. Meine ehrliche Antwort war: Sehr wenig. Die meisten Artikel, die ihren Weg in die Schweizer Tagespresse finden sind entweder irrelevant, masslos übertrieben oder fachlich schlicht und einfach falsch. Mein Gesprächspartner war etwas pikiert, hakte aber nach und fragte nach Ursachen. Meines Erachtens liegen diese nicht bei den Journalisten. Niemand kann von einem Journalisten erwarten, ein hochkomplexes Feld wie unseres vollumfänglich zu verstehen. Das Problem liegt an der Quelle – in unserer eigenen Industrie:

1. Übermässige Vereinfachung von Sachverhalten (“dumbing down”)
2. Mangel an kompetenten, qualifizierten Quellen/selbsternannte “Experten”
3. Das Anbieten falscher oder unzureichender Lösungen

Diese Gründe können mehr oder minder beliebig miteinander kombiniert werden. Beliebte Beispiel sind:

- Sicherheitsexperten reden von Bedrohungen, sprechen dabei aber nur von Viren, weil andere Angriffsvektoren erklärt werden müssten. Aus diesem Grund werden auch nur entsprechende Gegenmassnahmen (AV) empfohlen (1, 3)
- “Experten” warnen vor unermesslichen Risi-

ken epochalen Ausmasses und prophezeien den Untergang des Abendlandes (2, oft zu finden in Artikeln zu Stuxnet)
- Marketing-Mitarbeiter von "Sicherheitsfirmen", die Firewalls und AV-Produkte verkaufen, erklären wie man sich mit ihren Produkten gegen "Hackerangriffe" schützt (1, 2 und 3)

Es mag viele Motivationen geben, sich mit IT-Sicherheit zu beschäftigen. Einige profitieren sicherlich massiv von dieser Art von Berichterstattung. So mancher Hersteller einer "Sicherheitssoftware" hat sich mit geschickter Panikmache eine goldene Nase verdient. Fakt ist aber: Wir verlieren alle. Es existieren Risiken und Schwachstellen, über die wir informieren müssen und über die ein öffentlicher Dialog geführt werden muss – ohne Panikmache, sondern mit verständlichen und akkuraten Informationen zur Problematik.

Diesen Dialog zu starten, das ist die Aufgabe der professionellen IT-Security-Schaffenden. Wir müssen aufhören, still grollend zu akzeptieren, dass Probleme trivialisiert, inakkurat wiedergegeben oder mit falschen Empfehlungen versehen werden. Die, schweizerisch-sprichwörtliche "Faust im Sack" hilft niemanden weiter – aber der Dialog mit den Medienschaffenden und das Bereitstellen von akkuraten, verständlichen Informationen kann der erste Schritt dazu sein, das Thema IT-Sicherheit seriös und ernsthaft zu behandeln

5.2 Blog Digest Juni 2012

Der scip Blog Digest ist eine jeweils Ende des Monats erscheinende *Zusammenfassung* der wichtigsten, spannendsten und verrücktesten Beiträge aus der internationalen Blogosphäre. Mit der Durchsicht dieser Postings wird es einfach und unkompliziert möglich, in Bezug auf Entwicklungen im Bereich IT-Security auf dem Laufenden zu bleiben. Folgen Sie unserem Team auf Twitter, um jeweils die aktuellsten News zu erhalten.

- 10 Movie Scenes Of Authentication Worth Rewatching (darkreading.com)
- A bad couple of years for the cryptographic token industry (blog.cryptographyengineering.com)
- Algorithms: When is Random Really Random? (infosecisland.com)
- Android app steals contactless credit card data (scmagazine.com.au)
- Backup Security Best Practices (blogs.mcafee.com)
- Crypto breakthrough shows Flame was designed by world-class scientists (arstechnica.com)
- CVSS for Penetration Test Results (Part I) (blog.spiderlabs.com)
- Data Classification: Why it is Important for Information Security (infosecisland.com)
- Decoding Common XOR Obfuscation in Malicious Code (isc.sans.edu)
- Defeating Flame String Obfuscation with IDAPython (blog.spiderlabs.com)
- eHarmony Password Dump Analysis (blog.spiderlabs.com)
- Evolving Endpoint Malware Detection: Controls, Trade-offs and Compromises (securosis.com)
- Evolving Endpoint Malware Detection: Providing Context (securosis.com)
- Falsehoods programmers believe about networks (erratasec.blogspot.com)
- HashDos: 42% of IIS sites are still Vulnerable (devcentral.f5.com)
- How Advanced Malware Bypasses Process Monitoring (blog.fireeye.com)
- How Malicious Code Can Run in Microsoft Office Documents (blog.zeltser.com)
- How old is Flame? (labs.alienvault.com)
- JSLR (thespanner.co.uk)
- Kaspersky's Problematic Flame Analysis (jeffreycarr.blogspot.ch)
- Meet Flame, The Massive Spy Malware Infiltrating Iranian Computers (wired.com)
- Microsoft certification authority signing certificates added to the Untrusted Certificate Store (blogs.technet.com)
- Most Consumers Don't Understand Breach Notification (darkreading.com)
- Obama Order Sped Up Wave of Cyberattacks Against Iran (nytimes.com)
- Our password hashing has no clothes (troyhunt.com)
- Playing by the Rules: Performing Firewall Audits (resources.infosecinstitute.com)
- Protect answers to password reset questions with pen-and-paper (blog.eset.com)
- Rumor: LinkedIn Hacked – Password Hashes Dumped on Russian Forum (securityweek.com)
- Safe Browsing – Protecting Web Users for 5 Years and Counting (googleonlinesecurity.blogspot.com)
- Scientists crack RSA SecurID 800 tokens, steal cryptographic keys (arstechnica.com)
- Security warnings for suspected state-sponsored at-

tacks (googleonlinesecurity.blogspot.com)

- The Central Limit Theorem Makes Random Testing Hard (blog.regehr.org)
- Thoughts on Active Defense, Intrusion Deception, and Counterstrikes (securosis.com)
- Why Antivirus Companies Like Mine Failed to Catch Flame and Stuxnet (wired.com)
- XSS: Gaining access to HttpOnly Cookie in 2012 (seckb.yehg.net)

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:

Sean Rütschi
Security Consultant
T +41 44 404 13 13
seru-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!