Security-Webinar

Mai 2016

Dr. Christopher Kunz, filoo GmbH

Ihr Webinar-Team

filoo®
member of Thomas Krenn Group

- Referent: Dr. Christopher Kunz
  - CEO Hosting filoo GmbH / TK AG
  - Promotion IT Security
  - Vorträge auf Konferenzen
  - Autor von Artikeln & Büchern

- Moderation: Stefanie Jerchel
  - Marketing Thomas-Krenn.AG
  - Sammelt Fragen / Feedback

filoo GmbH

filoo®
member of Thomas Krenn Group

- Wir sind die Hosting-Tochter der Thomas-Krenn.AG
  - Sicheres, hochperformantes Hosting in Frankfurt
  - Mitarbeiter in Gütersloh und Freyung
- Primärer Rechenzentrumsstandort Frankfurt
  - Tier3, ISO 27001
  - Fläche in zwei Brandabschnitten
- Managed Services
  - Planung & Deployment
  - Security Services
  - Systemadministration

Agenda

filoo®
member of Thomas Krenn Group

- Security im April / Mai
  - OpenSSL
  - xtCommerce
  - QEMU VGA-Probleme
  - ImageTragick
  - Kryptotrojaner
  - Türkisches Datenleck
  - Badlock
  - Let‘s Encrypt
  - Tavis Ormandy vs. Trend Micro
- Wie funktioniert Bug-Disclosure?

OpenSSL

filoo®
member of Thomas Krenn Group

- Speicher-Adressierungsfehler beim Parsen von ASN.1 Datenstrukturen („Hoch“)
  - Behoben in OpenSSL im April 2015 – Sicherheitsfehler erst nachträglich entdeckt
- Fehler im Bugfix für Lucky-13 Angriff („Hoch“)
  - Bei bestimmten Cryptoalgorithmen kann ein MITM Traffic entschlüsseln
  - Behoben in OpenSSL 1.0.1t, 1.0.2h
- Diverse weitere („Low“)
  - Speicher-DoS, Stack-Disclosure, Heap corruption

xtCommerce Patch

filoo®
member of Thomas Krenn Group

- Sicherheitslücke in xtcommerce
  - 4.1.0
  - 4.1.1
  - 4.2.0
- Patch am 10.5. veröffentlicht – sollte sofort eingespielt werden
- Keine Exploit-Details
  - Mindestens ein XSS/CSRF
  - Session Hijacking
  - Paßwort-Handling

QEMU VGA Sorgen

filoo®
member of Thomas Krenn Group

- Fehler in der VGA-Emulation von QEMU
  - QEMU-VMs können außerhalb ihres designierten VGA-Speicherbereichs schreiben
  - Das kann zu Code-Ausführung im Host führen
- Anderer Fehler in VGA-Emulation erlaubt DoS
  - Crash des QEMU-Prozesses auf dem Host
- Aktuelle QEMU-Versionen bereits released
  - Betroffene Hosts ggf. einmal leeren/VMs neustarten

ImageTragick

filoo®
member of Thomas Krenn Group

- ImageMagick ist eine Bildverarbeitungsbibliothek
  - Beliebt auch bei Web-CMS
  - Implementationen für PHP, Ruby, Perl, etc.
- Manipulierte SVG/MVG Dateien können Code enthalten
  - Der wird dann beim Konvertieren ausgeführt
  - Etwa beim Hochladen von Bildern in ein CMS
- Auswirkungen
  - Dateien löschen/verschieben
  - HTTP-Requests auslösen
  - Dateien auslesen
- Mehr Infos: https://imagetragick.com/
- GraphicsMagick auch betroffen

Cryptotrojaner: BSI-Tips

filoo®
member of Thomas Krenn Group

- „Angemessen vorsorgen, im Schadensfall auf die Vorbereitungen zurückgreifen und NICHT zahlen.“
  - Anzeige erstatten
  - Betroffene Systeme vom Netz!
  - Infektionsvektor schließen
  - Systeme neu aufsetzen

- Maßnahmenpapier online
  - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Cyber-Sicherheit/Themen/Ransomware.pdf

Türkisches Datenleck

filoo®
member of Thomas Krenn Group

- Dump des türkischen Wählerverzeichnisses aufgetaucht
  - Daten von 2008
- Daten enthalten persönliche Informationen
  - Name + Namen der Eltern
  - Türkische Nationa—ID (TC Kimlik No)
  - Volle Adresse
- 6GB SQL-Dump mit 46,9M Einträgen
  - Das sind ca. 60% der Bevölkerung
- Motivation: Politischer Protest

Badlock

filoo®
member of Thomas Krenn Group

- Kritische Samba-/Windows-Lücke
- Man-in-the-Middle für SMB-Protokolle
  - Permissions auf Dateien und Verzeichnisse manipulieren
  - (Mit AD) AD-Einträge manipulieren, Services stoppen
- Denial of Service
- Fix:
  - Samba 4.4.2, 4.3.8, 4.2.11
  - Windows: Patchday 12.04.2016
  - Fixes beheben auch weitere Bugs

Let‘s Encrypt

filoo®
member of Thomas Krenn Group

- Let‘s Encrypt ist aus der Beta heraus
  - Über 1M Zertifikate ausgestellt
- Noch keine vertrauenswürdige CA
  - Zertifikate werden auch von IdenTrust signiert
  - Dadurch bei manchen Clients Probleme
- Beitritt im CA/Browser Forum
  - Zusammenschluß von CAs und Browser-Herstellern
  - Verwaltet Keystores vieler Browser
  - Klarer Schritt zur eigenen CA

Tavis O. vs. TrendmicrO

filoo®
member of Thomas Krenn Group

- Neue alte Probleme in TrendMicro AntiVirus:
  - Trend Micro Maximum Security
  - Trend Micro Premium Security
  - Trend Micro Password Manager
- Node.js Debugger-Instanz vergessen
  - Bindet sich an TCP-Port auf localhost
  - Kann per JavaScript angesprochen werden
  - <img src=javascript:localhost:40000>
  - Ausführung von beliebigen Programmen
- Patch wurde Ende März ausgerollt

Disclosure-Prozesse

filoo®
member of Thomas Krenn Group

- Sie haben einen sicherheitsrelevanten Bug gefunden
- Was tun?
- Drei grundsätzliche Modelle
  - No Disclosure
  - Responsible Disclosure
  - Full Disclosure

Non-Disclosure

filoo®
member of Thomas Krenn Group

- Sie behalten den Bug für sich
  - Nutzen ihn für einen eigenen Exploit
- Sie verkaufen den Bug an Dritte
  - Exploit-Hersteller
  - „Zero Day Initiative“ o.ä. – legale oder illegale Exploit-Händler
- Sie erzählen dem Hersteller davon
  - ...und lassen sich das bezahlen
- Alle Details bleiben geheim
- Funktioniert bei OpenSource nur ganz, ganz schlecht

Non-Disclosure: xtCommerce

filoo®
member of Thomas Krenn Group

- “Es gibt ein Problem, hier ist der Patch“
- Keine Details bekannt
- Per Diff kann man reverse engineeren
  - So arbeiten Exploit-Hersteller
- Exploit wird bald verfügbar sein

Coordinated Disclosure

filoo®
member of Thomas Krenn Group

- Sie besprechen das Problem mit dem Hersteller
  - Dieser erstellt einen Zeitplan
  - Erst wird gepatcht, dann ein Advisory veröffentlicht
  - Dieses kann Details enthalten
- Vorteile
  - Hersteller hat mehr Zeit zum Patchen
  - Skriptkiddies / Exploit-Herstellern wird Arbeit erschwert
- Nachteile
  - Andere haben mehr Zeit, den Exploit auszunutzen
  - Hersteller können Prozess beliebig verzögern / aussitzen

Coordinated Disclosure: OpenSSL

filoo®
member of Thomas Krenn Group

- Bugs wurden an OpenSSL gemeldet
- Dort wurde gepatcht
- Patch + Advisory wurden im Voraus angekündigt
- Nach Veröffentlichung: Details auf OpenSSL-Website

Full Disclosure

filoo®
member of Thomas Krenn Group

- Veröffentlichen von Lücken ohne Herstellerkontakt
  - Auf Mailinglisten wie full-disclosure
  - Im Web
- Oft mit sog. „PoC Exploit“
  - Einfacher Exploit, der das Problem aufzeigt
- Vorteile
  - Hersteller kommt unter Zugzwang
  - Extrem transparent, erleichtert Mitigation
- Nachteile
  - Exploit-Schreiber / Skriptkiddies starten sofort
  - Bei mancher Software: Nie Problembehebung

Full Disclosure: ImageMagick

filoo®
member of Thomas Krenn Group

- Bug gefunden – Vermutung: Andere haben ihn auch
- Bug ohne PoC veröffentlicht
- ImageMagick-Team reagiert
- Veröffentlichung von PoC unter imagetragick.org

Vorschau

filoo®
member of Thomas Krenn Group

_ Nächster Termin 15.06.2016

_ Ich freue mich auf Ihre Themenvorschläge!

Vielen Dank

filoo®
member of Thomas Krenn Group

- Ich freue mich auf Ihre Themenvorschläge und Fragen!

- Kontaktdaten:
  - E-Mail: chris@filoo.de
  - Telefon: 05241/86730-0

- Besuchen Sie filoo!
  - https://www.filoo.de/
  - http://twitter.com/filoogmbh