Security-Webinar

September 2016

Dr. Christopher Kunz, filoo GmbH

Ihr Webinar-Team

- Referent: Dr. Christopher Kunz
  - 1 / 2 Geschäftsführer filoo GmbH
  - Promotion IT Security
  - Vorträge auf Konferenzen
  - Autor von Artikeln & Büchern

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

filoo GmbH

- Hosting-Partner der Thomas-Krenn.AG
  - Seit September 2016 Teil der Adacor-Gruppe
  - Sicheres, hochperformantes Hosting in Frankfurt
- Primärer Rechenzentrumsstandort Frankfurt
  - Tier3, ISO 27001
  - Fläche in zwei Brandabschnitten
- Managed Services
  - Planung & Deployment
  - Security Services
  - Systemadministration

Agenda

filoo

- Security-Themen im Juli/August
  - Comodo CA-Probleme
  - WoSign CA-Probleme
  - MysQL Remote Root
  - VMWare Code Execution
  - Dropbox Paßwort-Leck
  - Cisco ASA Backdoor / Pixpocket

CA-Problem 1: Comodo

filoo

- Formular für Zertifikatsanträge („PositiveSSL Trial“) validierte falsch
  - HTML möglich
  - Damit kann die Bestätigungsmail manipuliert werden
  - „Click here“ versendet Bestätigungscode an Angreifer
- Lücke wurde am 6.6. an Comodo gemeldet
  - Fix am 25.7. spätestens deployed (Frühestens 1.7.)
  - Drei Wochen für so eine Lücke?

Comodo gefälschte Mail

ORDER #21758515 - Domain Control Validation for [redacted]

Inbox x

Comodo Security Services noreply_support@comodo.com via trust-provider.com 10:36 PM (2 minutes ago)

to me

Domain Control Validation for [redacted]

Dear mandatory@gmail.com,

We have received a request to issue an SSL certificate for:
Domain: [redacted]
Subject:

You have 24 hours to reject this request.

Click here to reject this request.

CA-Problem 2: WoSign

filoo

- WoSign ist eine chinesische CA
  - Kostenlose Zertifikate für jedermann
- Domainvalidierung fehlerhaft
  - Validierung für blah.domain.com beinhaltet domain.com
  - Wer eine Subdomain kontrolliert, kann Zertifikat für Hauptdomain erhalten
  - Außerdem: Validierung über Webserver auf hohem Port
- Fehlerhafte Zertifikate u.a. für github.com ausgestellt
- Nach Bekanntwerden zunächst Revocation verweigert
- Konsequenzen noch unklar

CA-Transparenz?

filoo

- WoSign ist „cross signed“ von StartCom
- Indizien für einen geheimen Kauf von StartCom durch WoSign mehren sich
- Whistleblower-Website mit rechtlichen Drohungen offline
- Und diesen Leuten sollen wir vertrauen?

MySQL Remote Root

filoo

- Verschiedene Lücken in MySQL gefunden
- Schreiben von Konfigurationsdateien in „unübliche“ Pfade
  - Notwendige Privilegien: SELECT, FILE
- Darüber .so-Bibliothek nachladen
  - Bibliothek räumt Config auf
  - Erstellt dann eine Connectback-Shell
- Root nach DB-Restart
- Kein offizielles Update von Oracle vorhanden
- Advisory mit PoC: http://legalhackers.com/advisories/MySQL-Exploit-Remote-Root-Code-Execution-Privesc-CVE-2016-6662.html

VMWare Code Execution

filoo

- DLL Hijacking bei Windows-Gästen
  - Ausführung beliebigen Codes
- HTTP Header-Injection in vCenter/ESXi
  - XSS, Script-/Redirect-Attacken
- Betroffen: vmWare Fusion, ESXi (5.0, 5.1, 5.5, 6.0)
  - https://www.vmware.com/security/advisories/VMSA-2016-0010.html

Dropbox Leak

- 68 Millionen Paßwörter geklaut
- Paßwörter sind echt & gehören alten Dropbox Accounts
- Benachrichtigung + Änderungsaufforderung von Dropbox versandt
- Paßwort lange nicht geändert: Jetzt tun!

ExtraBacon / Pixpocket

filoo

- ExtraBacon
  - Backdoor / Exploit für Cisco ASA Firewall Appliance
  - Buffer Overflow im SNMP, CVE-2016-6366
  - Remote Code Execution
  - Nur in IPv4 ausnutzbar
- Pixpocket
  - Exploit für Cisco PIX
  - Nutzt einen Buffer overread aus (ähnlich Heartbleed)
  - Firewall verrät dann u.U. VPN-Konfigurationen und –Schlüssel
- Exploits der Equation Group – Vermutlich NSA

Vorschau

filoo

- Nächster Termin: 16.11.
- Ich freue mich auf Ihre Themenvorschläge!

Vielen Dank

- 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