Was alles schief gehen kann - Anatomie einer Schwachstelle

Karlsruher Entwicklertag 2019
Karlsruhe, 03.06.2019

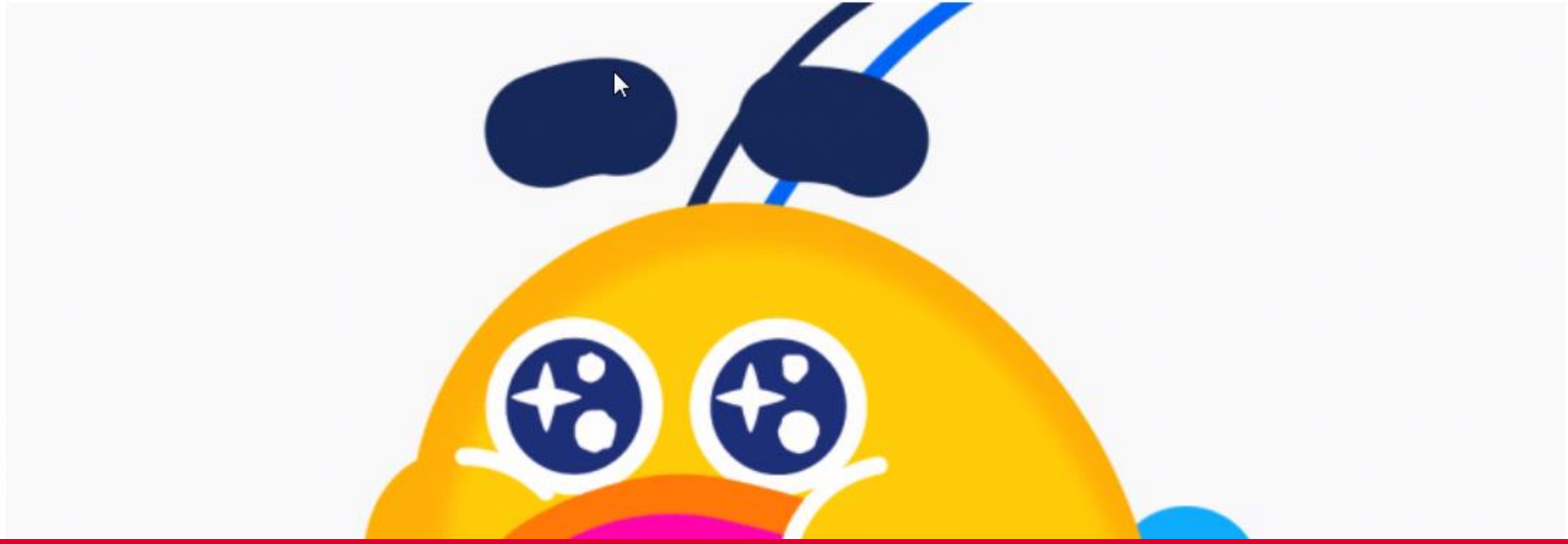
Hans-Joachim Knobloch, André Domnick

secorvo
security consulting

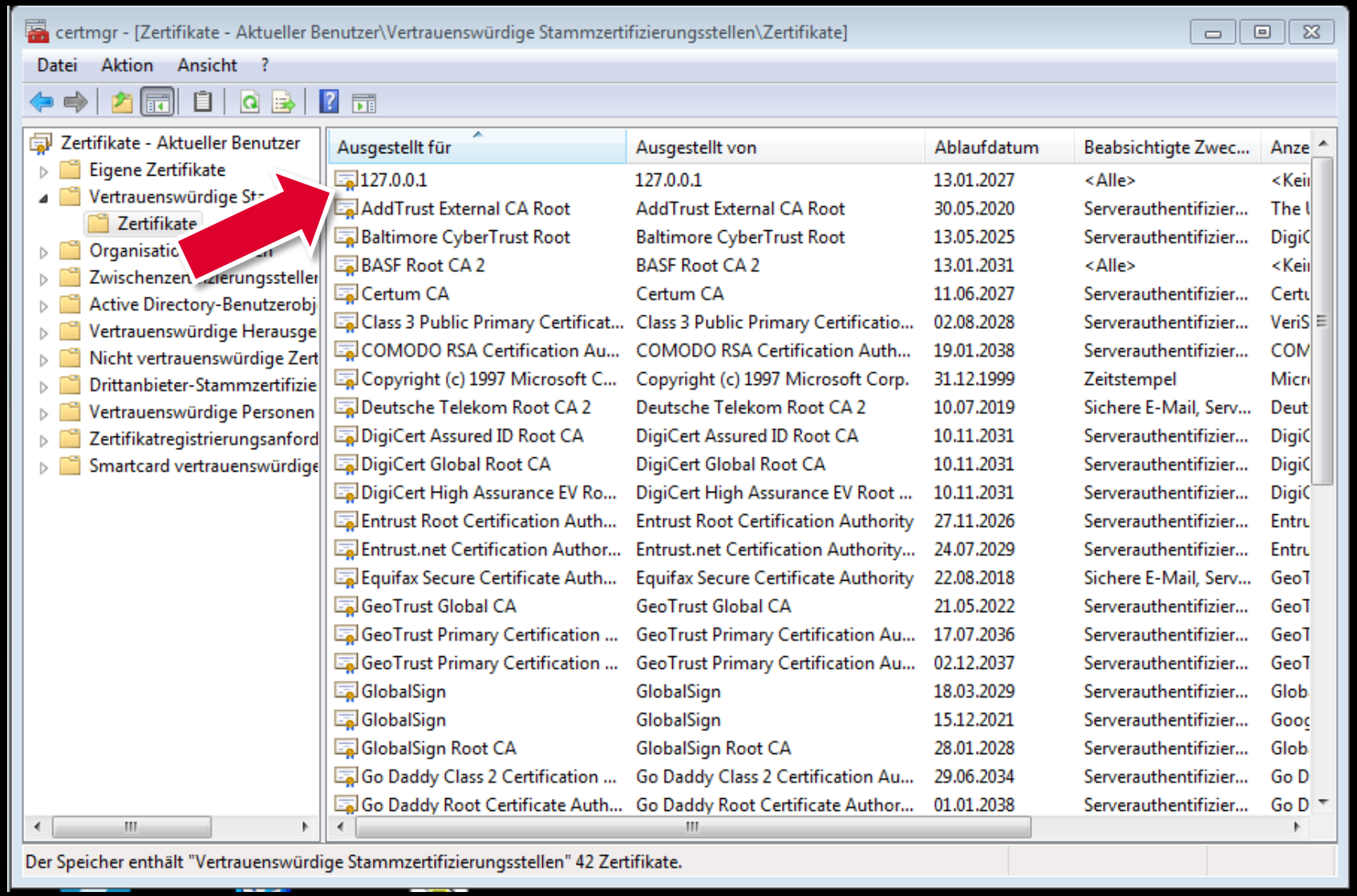
Wie Hersteller mit gemeldeten Schwachstellen umgehen

5 FEBRUARY 2019 / CYBERSEC

Researcher Assaulted By A Vendor After Disclosing A Vulnerability



20.07.2018 – Entdeckung



23.07. bis 08.08.2018 – Erste Kommunikation mit Sennheiser

03.09.2018 – Initiale Erwähnung in Secorvo Security News

Sennheisers Root-Zertifikat

Sennheiser Communications sorgte in diesem August bei manchen Anwendern der Software HeadSetup, die die Schnittstelle zwischen einem Sennheiser-Headset und dem Softphone bildet, für Unbehagen: Wird die Software installiert, so bringt diese huckepack ein vom Hersteller selbstsigniertes Root-Zertifikat mit, welches unbemerkt im Windows-Zertifikatspeicher als vertrauenswürdige Stammzertifizierungsstelle installiert wird. Damit nicht genug: Das Zertifikat trägt den „vertrauenswürdigen" Common Name 127.0.0.1. Der Aussteller des Zertifikats (oder ein Angreifer, der den zugehörigen Private Key erbeutet) kann damit Man-in-the-Middle-Angriffe auf mit TLS gesicherte Verbindungen beteiligter Systeme durchführen.

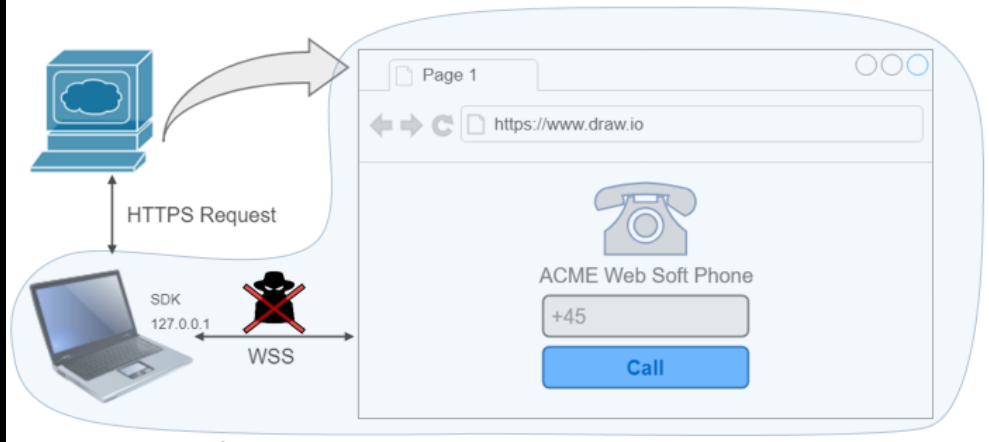
Dabei ist der Zweck des CA-Zertifikats unklar: Wir konnten keine negativen Folgen nach dem Löschen des ungebeten installierten Zertifikats feststellen. Bis Redaktionsschluss erhielten wir auch keine Antwort vom Hersteller auf die Frage nach dem Zweck dieser Maßnahme.

Dieser fahrlässige Umgang eines Herstellers mit der Sicherheit der IT-Infrastruktur der Kunden erinnert an Vorfälle wie Superfish auf Lenovo-PCs und -Laptops. Betroffenen empfehlen wir, Kontakt mit Sennheiser aufzunehmen und das Zertifikat aus dem Windows-Zertifikatspeicher zu entfernen.

13.09.2018 – Technische Begründung des Herstellers

Cross origin resource sharing (CORS) and Self-Signed Certificates

Explained



Above illustrates a PC / Laptop requesting a web page containing a web-based soft-phone, that communicates with SDK on the PC / Laptop, using Secure Web Sockets (WSS).

The reason behind using a self-signed certificate is to allow HTTPS / WWS requests to local-host from a web page.

This is because secure web pages does not allow requests to other origins, unless they are both trusted and secure. See. Same-origin policy https://en.wikipedia.org/wiki/Same-origin_policy

Note the following:

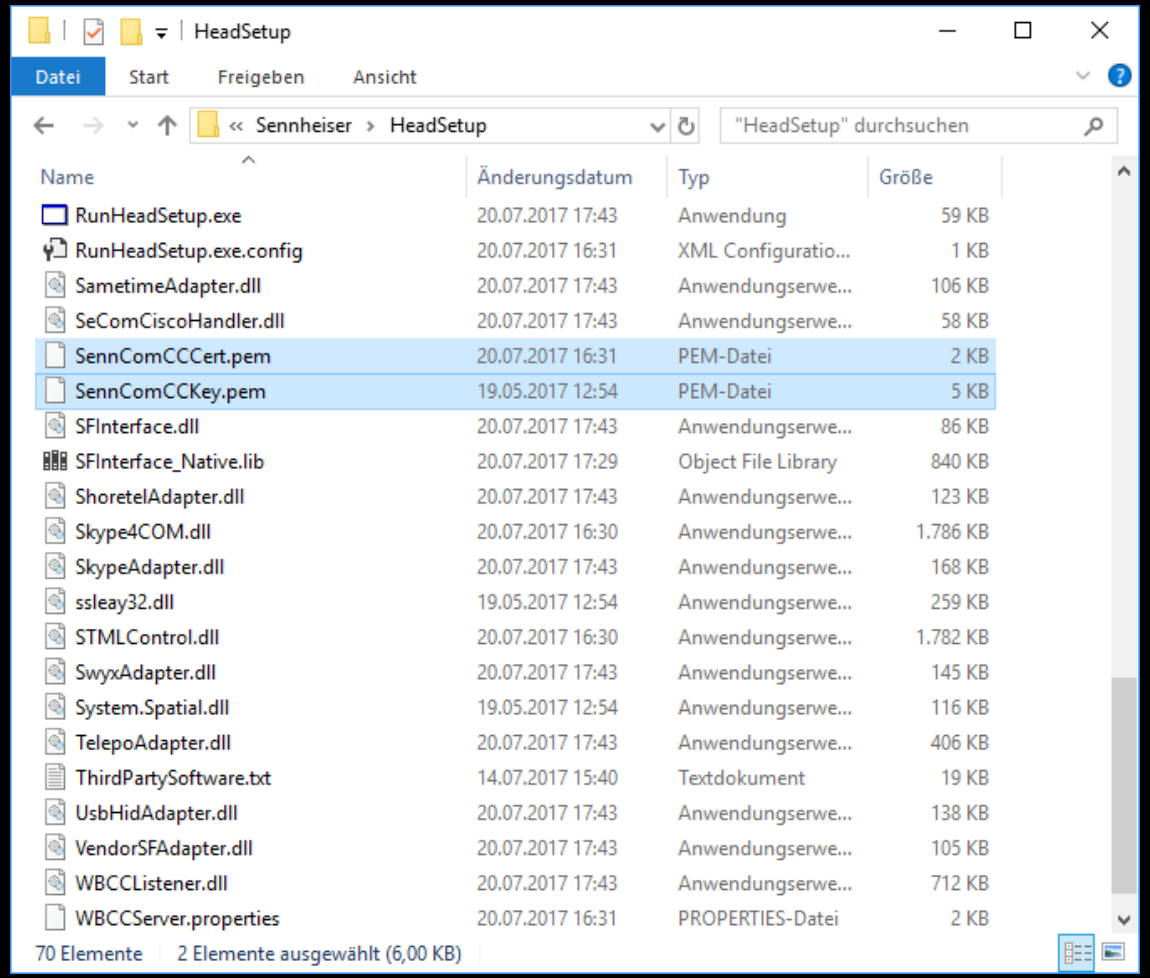
> *For absolute URIs, the origin is the triple {protocol, host, port}.....*
> *Two resources are considered to be of the same origin if and only if all these values are exactly the same.*

To mitigate the strict rules imposed by the same-origin policy, the CORS standard is applied to allow access to other origins, i.e. local host. See CORS https://en.wikipedia.org/wiki/Cross-origin_resource_sharing

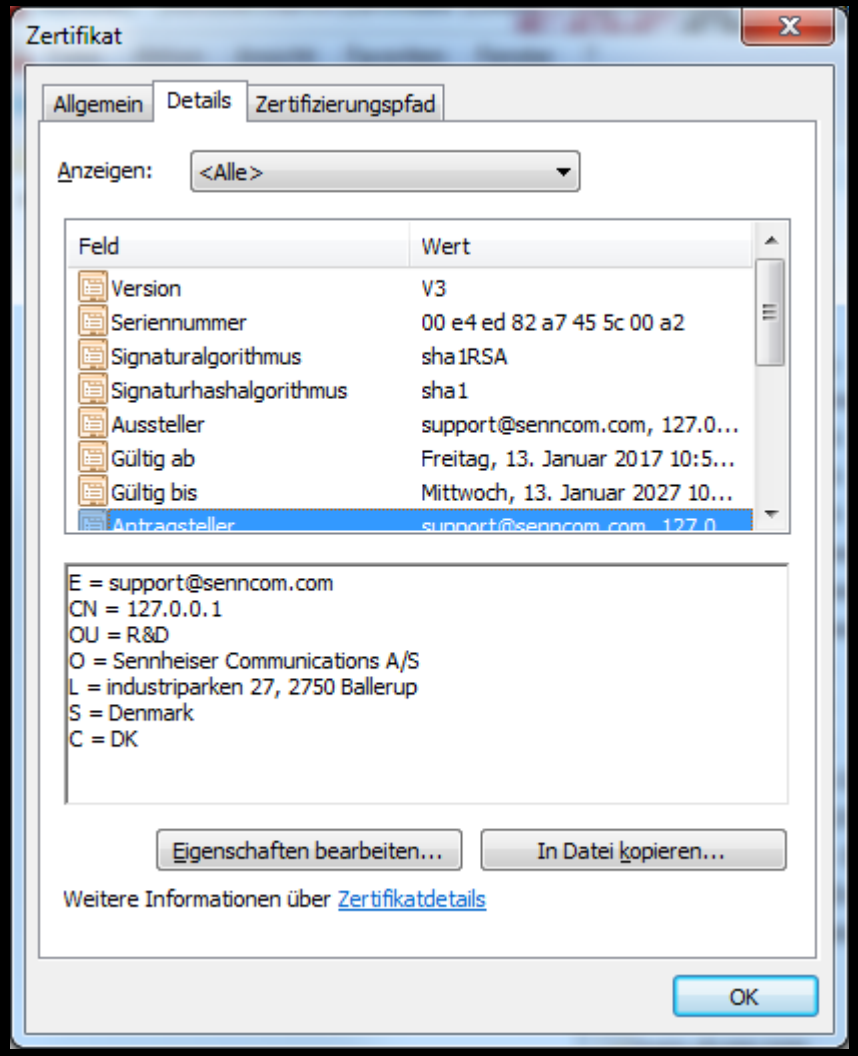
In this case the man in the middle is considered impossible or extremely difficult and unnecessary from a hacker's point of view, since it will require the hacker to gain administrative rights to the victim's computer in the first place.

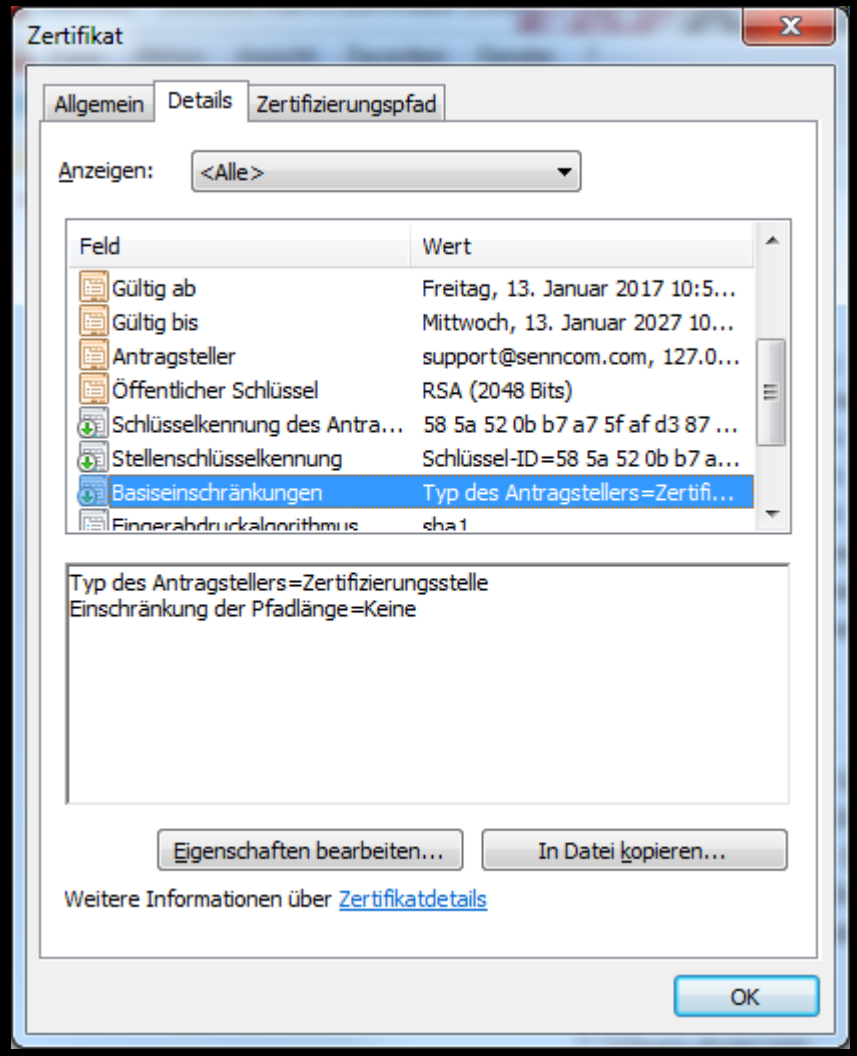
On the other hand, a hacker can attack by injecting code into a web server, the hacker will then be able to remote control the victim's browser and send requests to the SDK as call control commands, and gain the ability to

14.09. bis 21.09.2018 – Technische Analyse, Bericht, CVE



Details des Zertifikats





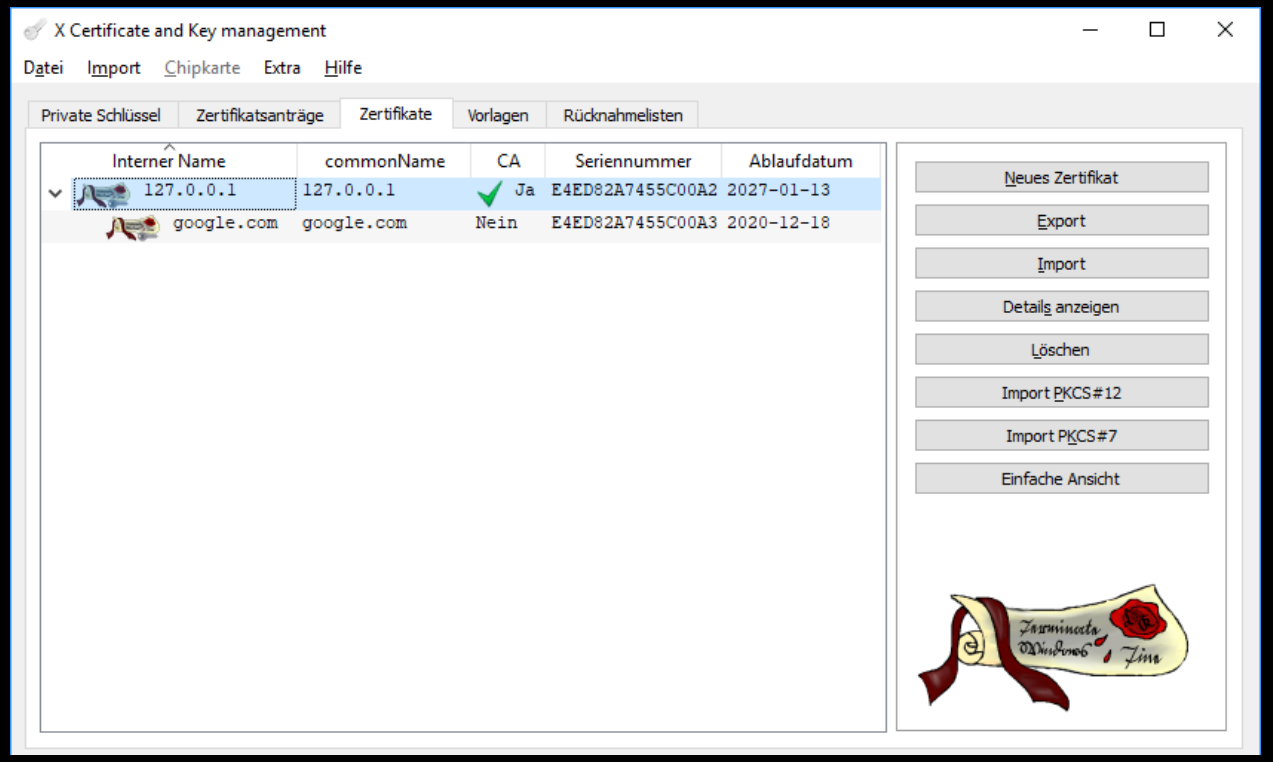
Deinstallation oder Update der Software entfernen die CA nicht!

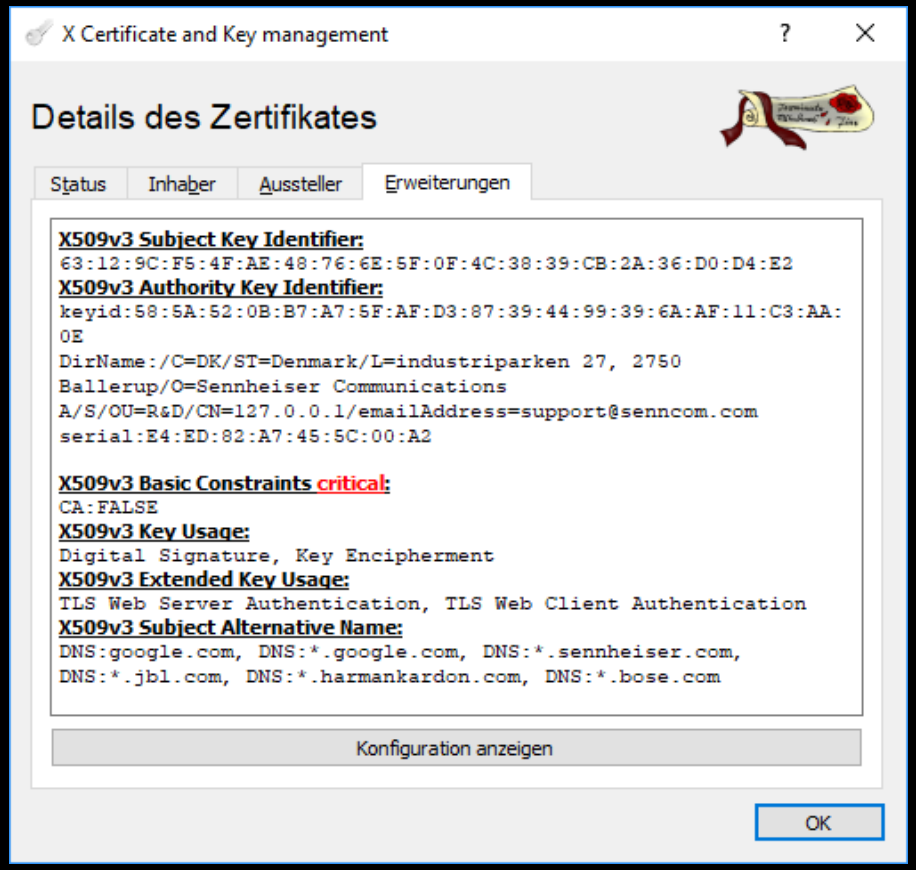
Extraktion des privaten Schlüssels

```
secorvo@ubuntu: /mnt/hgfs/File Lock/HeadSetup
secorvo@ubuntu:/mnt/hgfs/File Lock/HeadSetup$ strings WBCCListener.dll|grep -A 5
 -B 5 -i AES
resumecall
login-logout
SystemInformation
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
1234567890123456
aes-128-cbc
bad_weak_ptr
Generic transport policy error
websocketpp.transport
async_read_at_least call requested more bytes than buffer can store
Underlying Transport Error
secorvo@ubuntu:/mnt/hgfs/File Lock/HeadSetup$
```

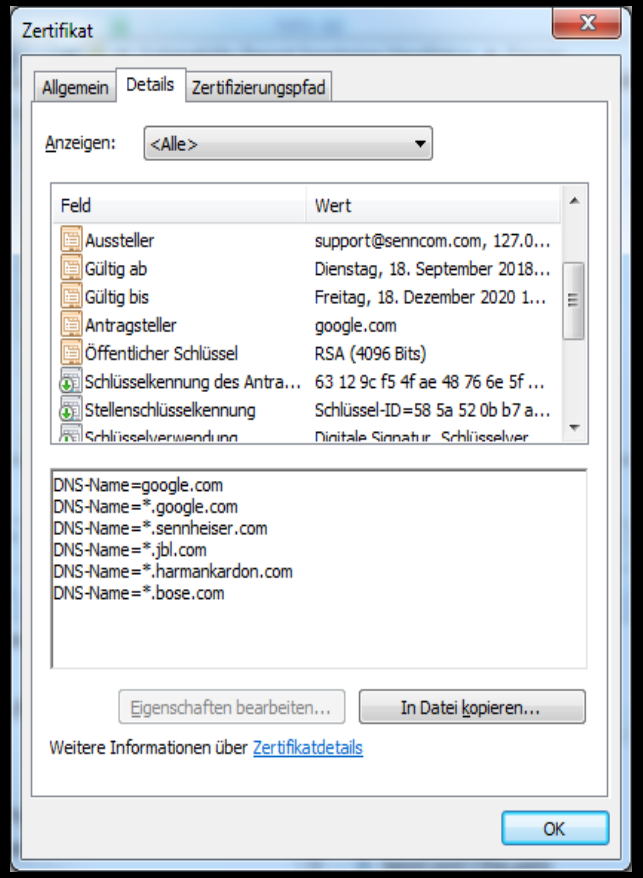
```
secorvo@ubuntu: /mnt/hgfs/File Lock/HeadSetup
secorvo@ubuntu:/mnt/hgfs/File Lock/HeadSetup$ grep -A5 -B5 -i pass WBCCServer.pr
operties
openSSL.server.caConfig = SennComCCCert.pem
openSSL.server.verificationMode = relaxed
openSSL.server.verificationDepth = 9
openSSL.server.loadDefaultCAFile = true
openSSL.server.cipherList = ALL:!ADH:!LOW:!EXP:!MD5:@STRENGTH
openSSL.server.privateKeyPassphraseHandler.name = KeyFileHandler
openSSL.server.privateKeyPassphraseHandler.options.password = SennheiserCC
openSSL.server.invalidCertificateHandler.name = AcceptCertificateHandler
openSSL.server.extendedVerification = false
openSSL.server.cacheSessions = true
openSSL.server.sessionIdContext = ${application.name}
openSSL.server.sessionCacheSize = 100
secorvo@ubuntu:/mnt/hgfs/File Lock/HeadSetup$
```

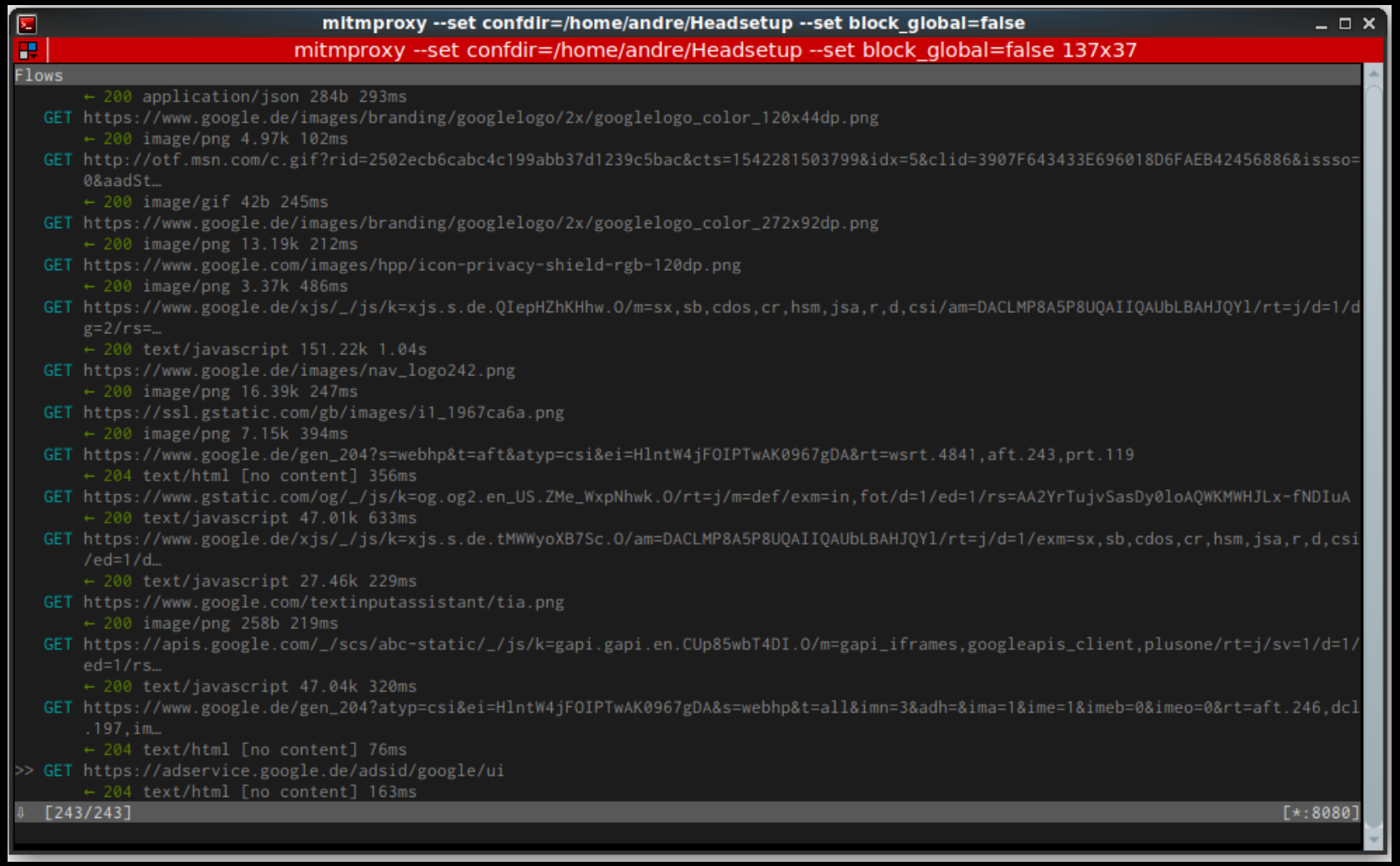
Ausstellen gefälschter Zertifikate

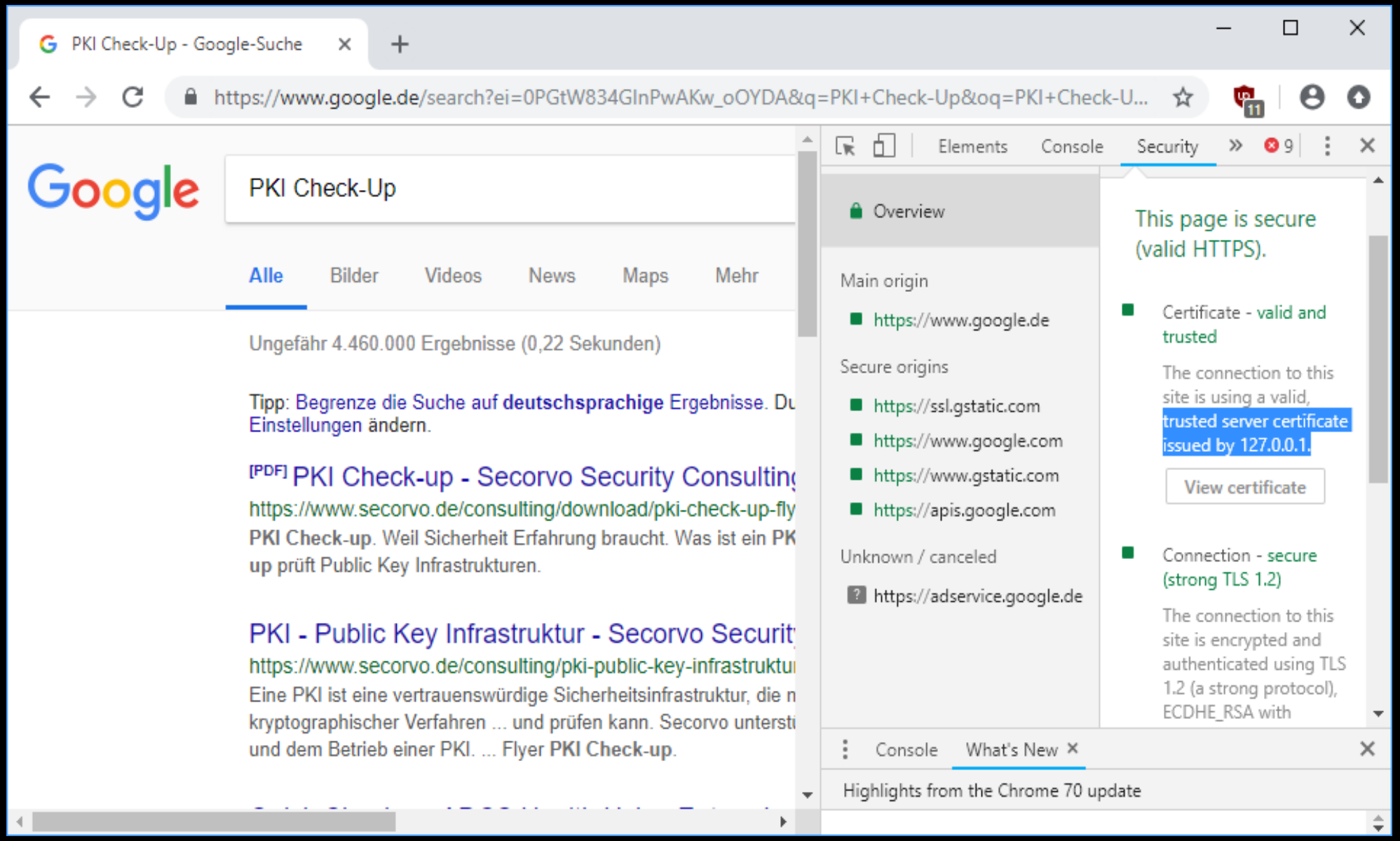




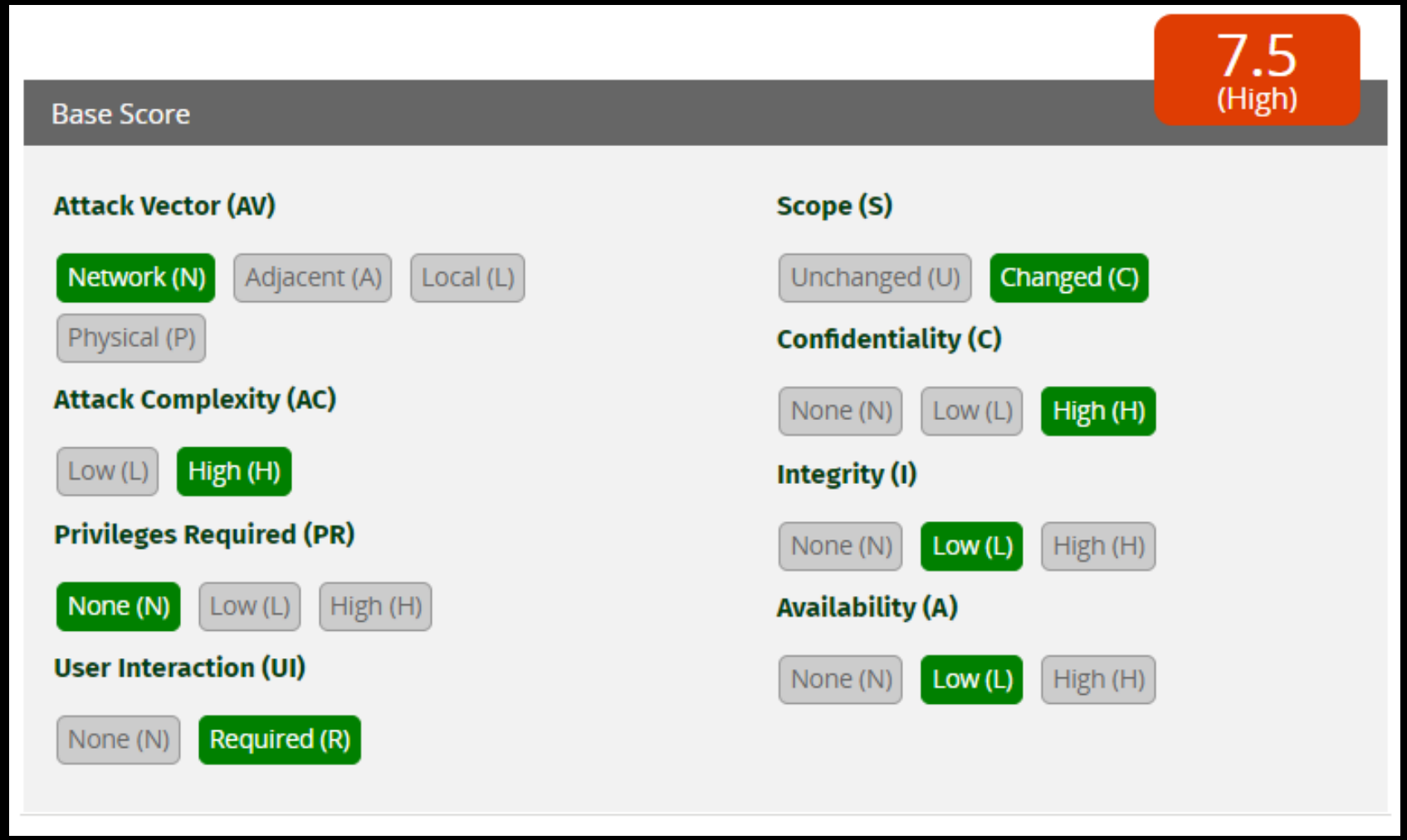
PoC mit Mitmproxy



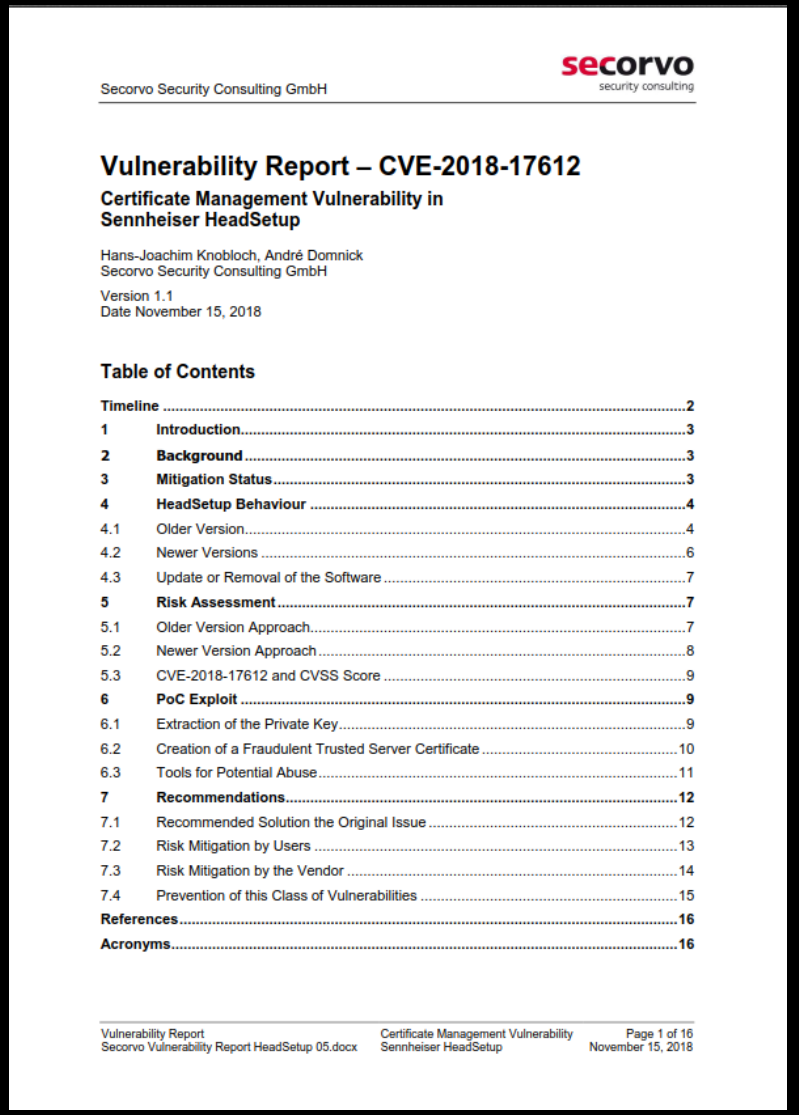



PKI Check-Up - Google-Suche
https://www.google.de/search?ei=0PGtW834GInPwAKw_oOYDA&q=PKI+Check-Up&oq=PKI+Check-U...
Google
PKI Check-Up
Alle
Bilder
Videos
News
Maps
Mehr
Ungefähr 4.460.000 Ergebnisse (0,22 Sekunden)
Tipp: Begrenze die Suche auf deutschsprachige Ergebnisse. Du
Einstellungen ändern.
[PDF] PKI Check-up - Secorvo Security Consulting
https://www.secorvo.de/consulting/download/pki-check-up-fly
PKI Check-up. Weil Sicherheit Erfahrung braucht. Was ist ein PK
up prüft Public Key Infrastrukturen.
PKI - Public Key Infrastruktur - Secorvo Securit
https://www.secorvo.de/consulting/pki-public-key-infrastruktu
Eine PKI ist eine vertrauenswürdige Sicherheitsinfrastruktur, die n
kryptographischer Verfahren ... und prüfen kann. Secorvo unterst
und dem Betrieb einer PKI. ... Flyer PKI Check-up.
Elements
Console
Security
9
Overview
Main origin
https://www.google.de
Secure origins
https://ssl.gstatic.com
https://www.google.com
https://www.gstatic.com
https://apis.google.com
Unknown / canceled
https://adservice.google.de
This page is secure (valid HTTPS).
Certificate - valid and trusted
The connection to this site is using a valid, trusted server certificate issued by 127.0.0.1.
View certificate
Connection - secure (strong TLS 1.2)
The connection to this site is encrypted and authenticated using TLS 1.2 (a strong protocol), ECDHE_RSA with
Console
What's New
Highlights from the Chrome 70 update

CVSSv3 Scoring



11.10.2018 – Bericht an Sennheiser, Antrag CVE



Vulnerability Report – CVE-2018-17612

Certificate Management Vulnerability in Sennheiser HeadSetup

Hans-Joachim Knobloch, André Domnick
Secorvo Security Consulting GmbH

Version 1.1
Date November 15, 2018

Table of Contents

26.10. bis 31.10.2018 – Kommunikation mit dem Hersteller

31.10.2018 – Veröffentlichung in den Security News

Secorvo Security News

Oktober 2018

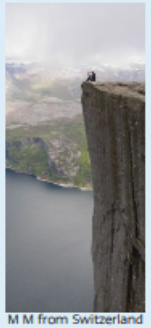
Rote Linien

Der Preikestolen ist ein Fels in der Nähe von Stavanger in Norwegen, der über 600 Meter senkrecht bis zum darunter liegenden Fjord abfällt. Hunderttausende besichtigen jährlich dieses Naturwunder. Aber keiner der Besucher, der noch bei Sinnen ist, käme auf die Idee, von dort im Wingsuit hinunter zu springen, ohne über ein gerüttelt Maß an Erfahrung als Fallschirmspringer zu verfügen.

Beim Software-Entwurf sind die roten Linien, die man tunlichst nicht überschreiten sollte, meist nicht ganz so leicht zu erkennen wie die Kante des Preikestolen. Und die möglichen Leidtragenden sind in der Regel die Anwender – und nicht die Entwickler, die die Linie überschreiten. Oft, oder besser: allzu oft verändern Designer einer Anwendung übergreifende Rechteeinstellungen des Systems, hantieren mit hoch privilegierten Benutzern und deren Credentials oder – so wie die in diesen Security News beschriebene Headset-Software – schieben dem System ein Root-Zertifikat unter, dessen Schlüssel sie gleich mit ausliefern. In solchen Fällen sollte man jedoch mindestens zweimal überlegen, ob man nicht auch ans Ziel kommt, ohne diese Linie zu überschreiten.

Wer sich dennoch in derart unsichere Gefilde begibt, der sollte beizeiten Experten für dieses Territorium hinzuziehen, die ein unabhängiges Design-Review durchführen. Zwar kann selbst dann noch etwas schief gehen – so wie leider nur zu oft auch bei Extremsportlern in Wingsuits – aber ohne eigene Erfahrung ist das Risiko unkalkulierbar und ein Scheitern wahrscheinlich.

Und noch etwas können Entwickler von Extremsportlern lernen: Hinter sich aufzuräumen und beim Gehen die Umgebung hinter der roten Linie so zurückzulassen, wie man sie vorgefunden hat.



M M from Switzerland (CC-BY-SA 2.0)

Sennheisers HeadSetup revisited

In den SSN 08/2018 warnten wir vor dem fahrlässigen Umgang der Software Sennheiser HeadSetup mit CA-Zertifikaten. Anschließend analysierten wir einige ältere Versionen der betroffenen Software genauer – und dabei zeigte sich, dass die Schwachstelle gravierender ist als ursprünglich angenommen. Denn mit Informationen aus der Anwendung konnte auch der geheime CA-Schlüssel ausgelesen und missbraucht werden. Als „Proof of Concept" realisierten wir mit der Root-CA einen Man-in-the-Middle-Angriff auf TLS-Verbindungen und hebelten so die HTTPS-Verschlüsselung aus: Die Schwachstelle untergräbt für betroffene Systeme die gesamte zertifikatsbasierte Vertrauensinfrastruktur.

Im Gespräch mit dem Hersteller stellte sich heraus, dass die CA lediglich genutzt wird, um vertrauenswürdige Serverzertifikate für den lokal betriebenen Websocket-Dienst bereitzustellen. Dieser Dienst soll Schnittstellen zwischen Headset und Web-basierten Softphones implementieren. Dafür hätte es jedoch keiner eigenen Root-CA bedurft.

Als sei das noch nicht genug, unterliefen dem Hersteller in seinem Deinstallations- bzw. Update-Programm weitere Fehler: So werden die nicht mehr benötigten CA-Zertifikate nicht aus dem Zertifikatsspeicher von Windows entfernt. Alle Systeme, auf denen irgendwann eine der von der Schwachstelle betroffenen Versionen von HeadSetup installiert war, sind daher weiterhin angreifbar – obwohl jüngere Versionen von HeadSetup mittlerweile eine nicht so einfach zu missbrauchende CA nutzen.

05.11.2018 – Hinweis an Heise und Golem

09.11.2018 – Golem und Heise berichten

ROOT-ZERTIFIKAT

Sennheiser-Software hebelt HTTPS-Sicherheit aus

Eine Software für Headsets des Herstellers Sennheiser installiert ein Root-Zertifikat und sorgt damit dafür, dass HTTPS-Verbindungen nicht mehr sicher sind. In neueren Versionen ist die Lücke etwas weniger schlimm, einen Fix gibt es bisher nicht.

9. November 2018, 7:00 Uhr, Hanno Böck

(Bild: Sennheiser)

Eine Software zur Verwaltung von Sennheiser-Headsets kommt mit einer gravierenden Sicherheitslücke.

heise Security

News ▾ Hintergrund Events

Security > 7-Tage-News > 11/2018 > Sennheiser-Software spielt Angreifern mächtige Werkzeuge in die Hände

Sennheiser-Software spielt Angreifern mächtige Werkzeuge in die Hände UPDATE

Stand: 09.11.2018 12:02 Uhr – Dennis Schirrmacher

(Bild: TheDigitalArtist)

Die HeadSetup-Software von Sennheiser hinterlegt in Windows Root-Zertifikate mitsamt einem privaten Schlüssel. Das könnten Angreifer missbrauchen.

Sennheisers HeadSetup-Software reißt eine Sicherheitslücke (CVE-2018-17612) in Windows und Angreifer könnten sich in bestimmten Situationen als Man in the Middle in verschlüsselte HTTPS-Verbindungen einklinken. Der Bedrohungsgrad ist mit "hoch" eingestuft (CVSS v3 Base Score 7.5 von 10).

Veröffentlichung CVE-Eintrag

CVE-ID	
CVE-2018-17612	Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information

Description

Sennheiser HeadSetup 7.3.4903 places Certification Authority (CA) certificates into the Trusted Root CA store of the local system, and publishes the private key in the SennComCCKey.pem file within the public software distribution, which allows remote attackers to spoof arbitrary web sites or software publishers for several years, even if the HeadSetup product is uninstalled. NOTE: a vulnerability-assessment approach must check all Windows systems for CA certificates with a CN of 127.0.0.1 or SennComRootCA, and determine whether those certificates are unwanted.

References

Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- MISC:https://www.secorvo.de/publikationen/headsetup-vulnerability-report-secorvo-2018.pdf

Assigning CNA

MITRE Corporation

Date Entry Created	
20180928	Disclaimer: The entry creation date may reflect when the CVE ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

Phase (Legacy)

Assigned (20180928)

12.11.2018 – Reaktion von Sennheiser

HeadSetup & HeadSetup Pro software are temporarily not available for download due to a potential security threat.

The software stores certificates in the certificate storage, unfortunately these certificates are vulnerable. We are currently working on a software update to solve the issue. The update will be made available from beginning of calendar week 47. The embedded software in the headsets is not affected, and headsets can be used without the "HeadSetup" software.

As an immediate remedy users can remove the affected certificates from the certificate storage by downloading following.

To remove the affected certificates from one individual computer - Please download the script.

After running the script with administrative privileges, the risk of Sennheiser certificates being subject for misuse will be eliminated. The file also includes a description on how users can manually verify that certificates are removed.
For business users, it is advised to use the AD/GPO process instead.

Download remove certificates file >

Download this pdf Step-by-Step guide for how to move the affected Sennheiser certificates to the untrusted certificate Active Directory (AD) – Group Policy (GPO)

This will eliminate the risk of Sennheiser certificates being subject for misuse.

For PC users:
Download step-by-step guide >

For MAC users:
Download step-by-step guide >

As deinstallation of the software "HeadSetup" alone does not resolve the situation, we recommend that also customers remove the vulnerable ceritificates, who no longer actively use the add-on software.

All former and current users may contact Sennheiser Communications for support: help@senncom.com or at +45 2943 1569 (9.00-18.00 CET)

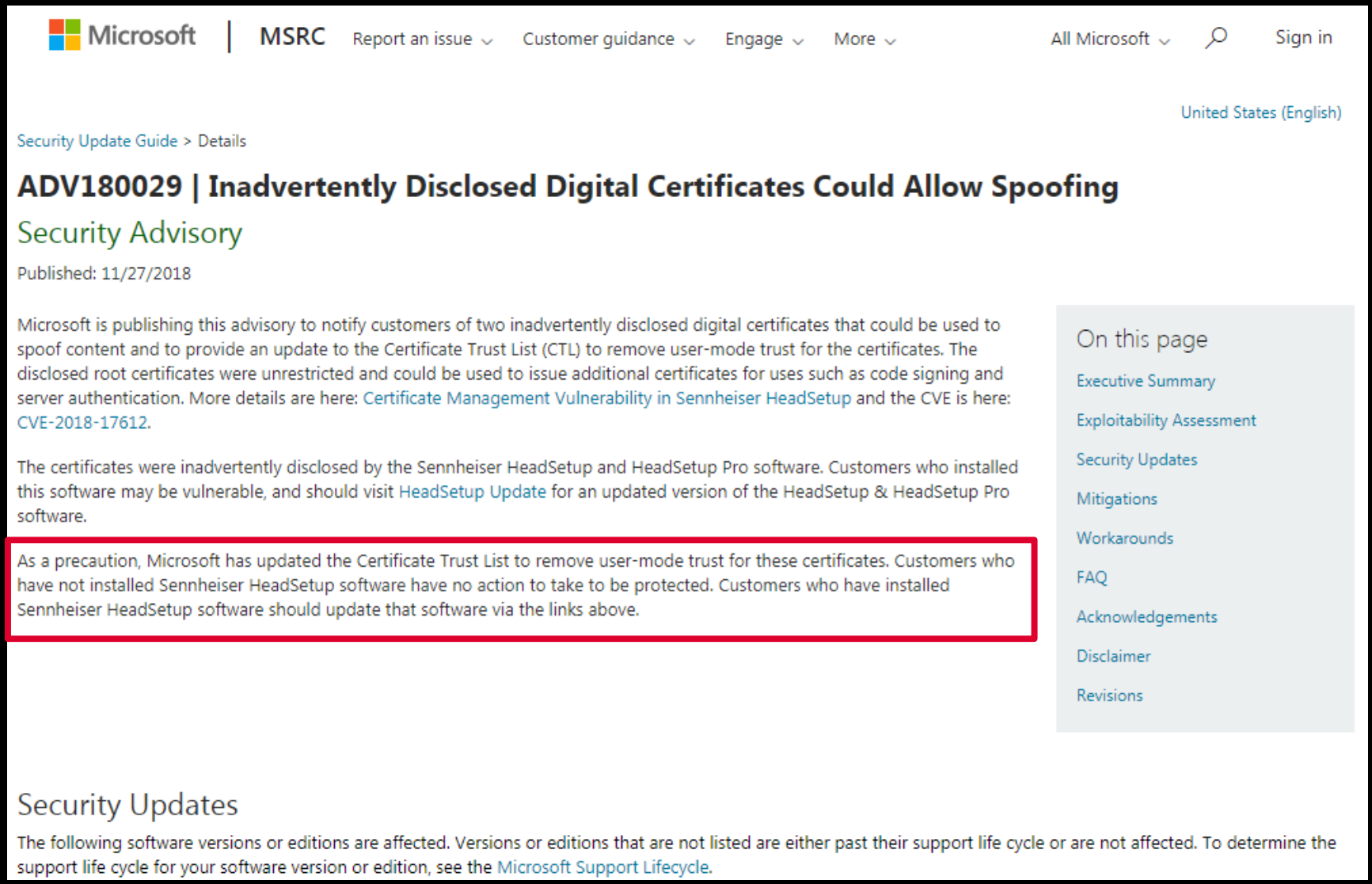
23.11.2018 – Sennheiser veröffentlich aktualisierte Software

Headsetup and Headsetup Pro Update.
Following a vulnerability identified in Sennheiser Headsetup and Headsetup Pro on November 9, new versions of all software have been made available.

Updating the software to its latest version will rid the software of vulnerable certificates.
As of a November 23 update, the latest software versions are as follows: Headsetup Pro v.2.6.8235; Headsetup: v.8.1.6114 (for PC) and v. 5.3.7011 (for Mac). Available for download below.

All users may contact Sennheiser Communications for support: **help@senncom.com** or at +45 2943 1569 (9.00-18.00 CET)

27.11.2018 – Microsoft Security Advisory



Microsoft | MSRC Report an issue Customer guidance Engage More All Microsoft Sign in

United States (English)

Security Update Guide > Details

ADV180029 | Inadvertently Disclosed Digital Certificates Could Allow Spoofing

Security Advisory

Published: 11/27/2018

Microsoft is publishing this advisory to notify customers of two inadvertently disclosed digital certificates that could be used to spoof content and to provide an update to the Certificate Trust List (CTL) to remove user-mode trust for the certificates. The disclosed root certificates were unrestricted and could be used to issue additional certificates for uses such as code signing and server authentication. More details are here: Certificate Management Vulnerability in Sennheiser HeadSetup and the CVE is here: CVE-2018-17612.

The certificates were inadvertently disclosed by the Sennheiser HeadSetup and HeadSetup Pro software. Customers who installed this software may be vulnerable, and should visit HeadSetup Update for an updated version of the HeadSetup & HeadSetup Pro software.

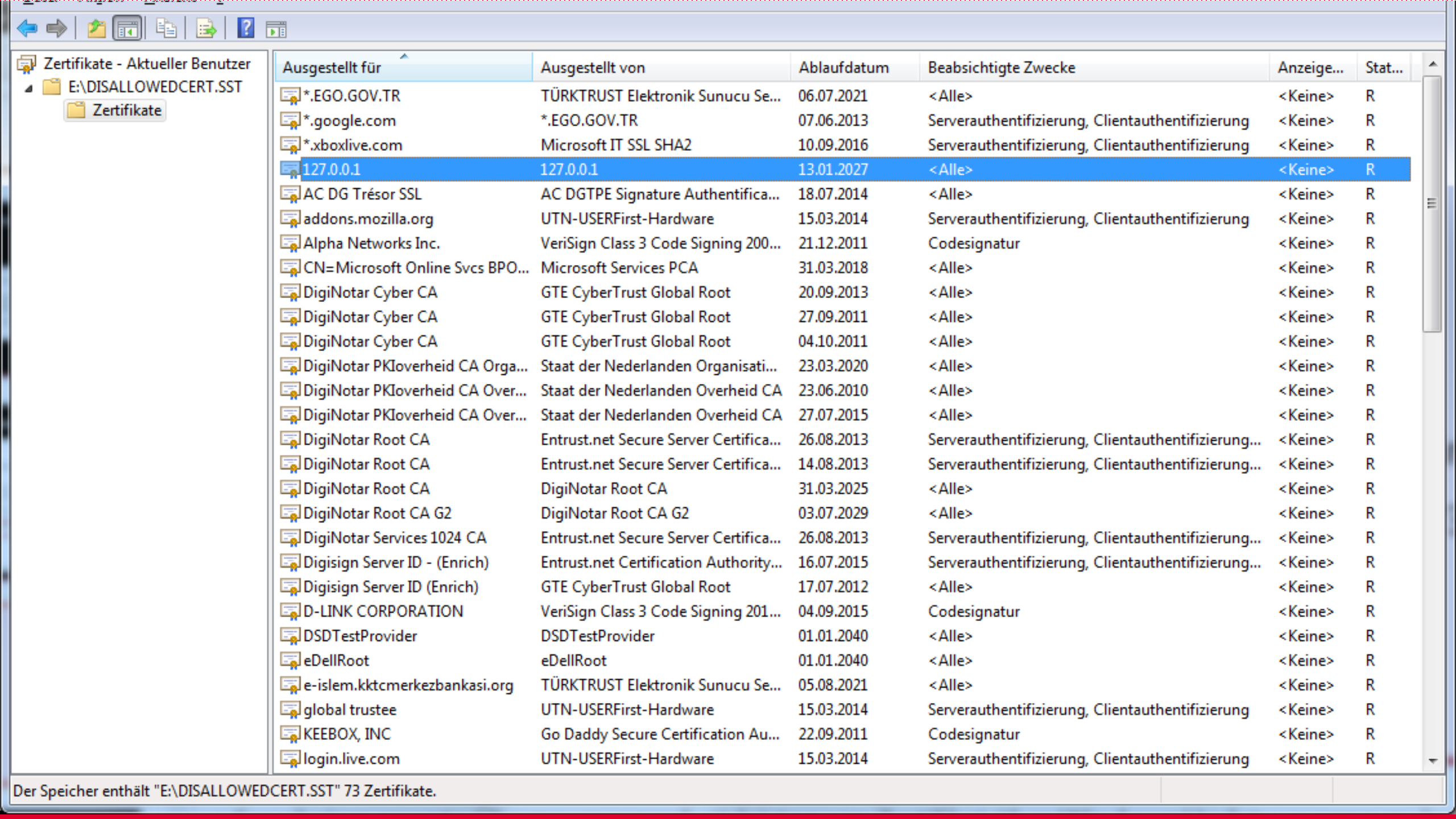
As a precaution, Microsoft has updated the Certificate Trust List to remove user-mode trust for these certificates. Customers who have not installed Sennheiser HeadSetup software have no action to take to be protected. Customers who have installed Sennheiser HeadSetup software should update that software via the links above.

On this page

Executive Summary
Exploitability Assessment
Security Updates
Mitigations
Workarounds
FAQ
Acknowledgements
Disclaimer
Revisions

Security Updates

The following software versions or editions are affected. Versions or editions that are not listed are either past their support life cycle or are not affected. To determine the support life cycle for your software version or edition, see the Microsoft Support Lifecycle.


Zertifikate - Aktueller Benutzer
E:\DISALLOWEDCERT.SST
Zertifikate
Ausgestellt für
Ausgestellt von
Ablaufdatum
Beabsichtigte Zwecke
Anzeige...
Stat...
*.EGO.GOV.TR
TÜRKTRUST Elektronik Sunucu Se...
06.07.2021
<Alle>
<Keine>
R
*.google.com
*.EGO.GOV.TR
07.06.2013
Serverauthentifizierung, Clientauthentifizierung
<Keine>
R
*.xboxlive.com
Microsoft IT SSL SHA2
10.09.2016
Serverauthentifizierung, Clientauthentifizierung
<Keine>
R
127.0.0.1
127.0.0.1
13.01.2027
<Alle>
<Keine>
R
AC DG Trésor SSL
AC DGTPE Signature Authentifica...
18.07.2014
<Alle>
<Keine>
R
addons.mozilla.org
UTN-USERFirst-Hardware
15.03.2014
Serverauthentifizierung, Clientauthentifizierung
<Keine>
R
Alpha Networks Inc.
VeriSign Class 3 Code Signing 200...
21.12.2011
Codesignatur
<Keine>
R
CN=Microsoft Online Svcs BPO...
Microsoft Services PCA
31.03.2018
<Alle>
<Keine>
R
DigiNotar Cyber CA
GTE CyberTrust Global Root
20.09.2013
<Alle>
<Keine>
R
DigiNotar Cyber CA
GTE CyberTrust Global Root
27.09.2011
<Alle>
<Keine>
R
DigiNotar Cyber CA
GTE CyberTrust Global Root
04.10.2011
<Alle>
<Keine>
R
DigiNotar PKIoverheid CA Orga...
Staat der Nederlanden Organisati...
23.03.2020
<Alle>
<Keine>
R
DigiNotar PKIoverheid CA Over...
Staat der Nederlanden Overheid CA
23.06.2010
<Alle>
<Keine>
R
DigiNotar PKIoverheid CA Over...
Staat der Nederlanden Overheid CA
27.07.2015
<Alle>
<Keine>
R
DigiNotar Root CA
Entrust.net Secure Server Certifica...
26.08.2013
Serverauthentifizierung, Clientauthentifizierung...
<Keine>
R
DigiNotar Root CA
Entrust.net Secure Server Certifica...
14.08.2013
Serverauthentifizierung, Clientauthentifizierung...
<Keine>
R
DigiNotar Root CA
DigiNotar Root CA
31.03.2025
<Alle>
<Keine>
R
DigiNotar Root CA G2
DigiNotar Root CA G2
03.07.2029
<Alle>
<Keine>
R
DigiNotar Services 1024 CA
Entrust.net Secure Server Certifica...
26.08.2013
Serverauthentifizierung, Clientauthentifizierung...
<Keine>
R
Digisign Server ID - (Enrich)
Entrust.net Certification Authority...
16.07.2015
Serverauthentifizierung, Clientauthentifizierung...
<Keine>
R
Digisign Server ID (Enrich)
GTE CyberTrust Global Root
17.07.2012
<Alle>
<Keine>
R
D-LINK CORPORATION
VeriSign Class 3 Code Signing 201...
04.09.2015
Codesignatur
<Keine>
R
DSDTestProvider
DSDTestProvider
01.01.2040
<Alle>
<Keine>
R
eDellRoot
eDellRoot
01.01.2040
<Alle>
<Keine>
R
e-islem.kktcmerkezbankasi.org
TÜRKTRUST Elektronik Sunucu Se...
05.08.2021
<Alle>
<Keine>
R
global trustee
UTN-USERFirst-Hardware
15.03.2014
Serverauthentifizierung, Clientauthentifizierung
<Keine>
R
KEEBOX, INC
Go Daddy Secure Certification Au...
22.09.2011
Codesignatur
<Keine>
R
login.live.com
UTN-USERFirst-Hardware
15.03.2014
Serverauthentifizierung, Clientauthentifizierung
<Keine>
R
Der Speicher enthält "E:\DISALLOWEDCERT.SST" 73 Zertifikate.

Weitere Medien springen auf den Zug auf

Gesammelte Pressemeldungen

https://www.secorvo.de/presse/index.html

Dezember 2018: Podcast: Security Now – Folgen: 692, 693

Exkurs: Umgang mit Mixed Content

Mixed Content

Editor's Draft, 19 June 2018

This version:
https://w3c.github.io/webappsec-mixed-content/

Latest published version:
https://www.w3.org/TR/mixed-content/

Previous Versions:
https://www.w3.org/TR/2015/CR-mixed-content-20160802/

Version History:
https://github.com/w3c/webappsec-mixed-content/commits/master/index.src.html

Feedback:
public-webappsec@w3.org with subject line "`[mixed-content]` … *`message topic`* …" (archives)

Editor:
Mike West (Google Inc.)

Participate:
File an issue (open issues)

Abstract

This specification describes how a user agent should handle fetching of content over unencrypted or unauthenticated connections in the context of an encrypted and authenticated document.

Mixed Content

Ist das Mixed Content?

Allow `http://127.0.0.1`. #4

Closed **mikewest** opened this issue on 29 Apr 2016 · 0 comments

mikewest commented on 29 Apr 2016 — Member

Currently, mixed content checks block `http://127.0.0.1` from loading in a page delivered over TLS. I'm (belatedly) coming around to the idea that that restriction does more harm than good. In particular, I'll note that folks are installing new trusted roots and self-signing certs for that IP address, exposing themselves to additional risk for minimal benefit. Helpful locally installed software is doing the same, with even more associated risk.

I'd like to change MIX to use the Secure Contexts spec's notion of "potentially trustworthy" origins as opposed to toggling strictly based on the URL's protocol. This would be a normative change that would force us back to CR again. *shrug* Seems like it might be worth doing anyway.

👍 4

mikewest closed this in `349501c` on 20 Jul 2016

Assignees

No one assigned

Labels

None yet

Projects

None yet

Milestone

No milestone

1 participant

Use 'Is URL trustworthy?' rather than whitelisting 'https' and 'wss'.

Browse files

```
Based on the discussion in the public-webappsec thread starting at [1],
our face-to-face at [2], and our recent call at [3], this patch aligns
mixed content's checks with Secure Context's definition of potentially
trustworthy URLs.

Among other things, this means that `http://127.0.0.1/` will not be
considered mixed content when loaded in an otherwise secure page.

[1]: https://lists.w3.org/Archives/Public/public-webappsec/2016Apr/0044.html
[2]: https://www.w3.org/2016/05/16-webappsec-minutes.html#item05
[3]: https://www.w3.org/2016/07/13-webappsec-minutes.html#item05

Closes #4.
Obviates #5.
```

master

mikewest committed on 20 Jul 2016 1 parent 2ed0d54 commit 349501cdaa4b4dc1e2a8aacb216ced58fd316165

Showing 1 changed file with **26 additions** and **8 deletions**.

Unified Split

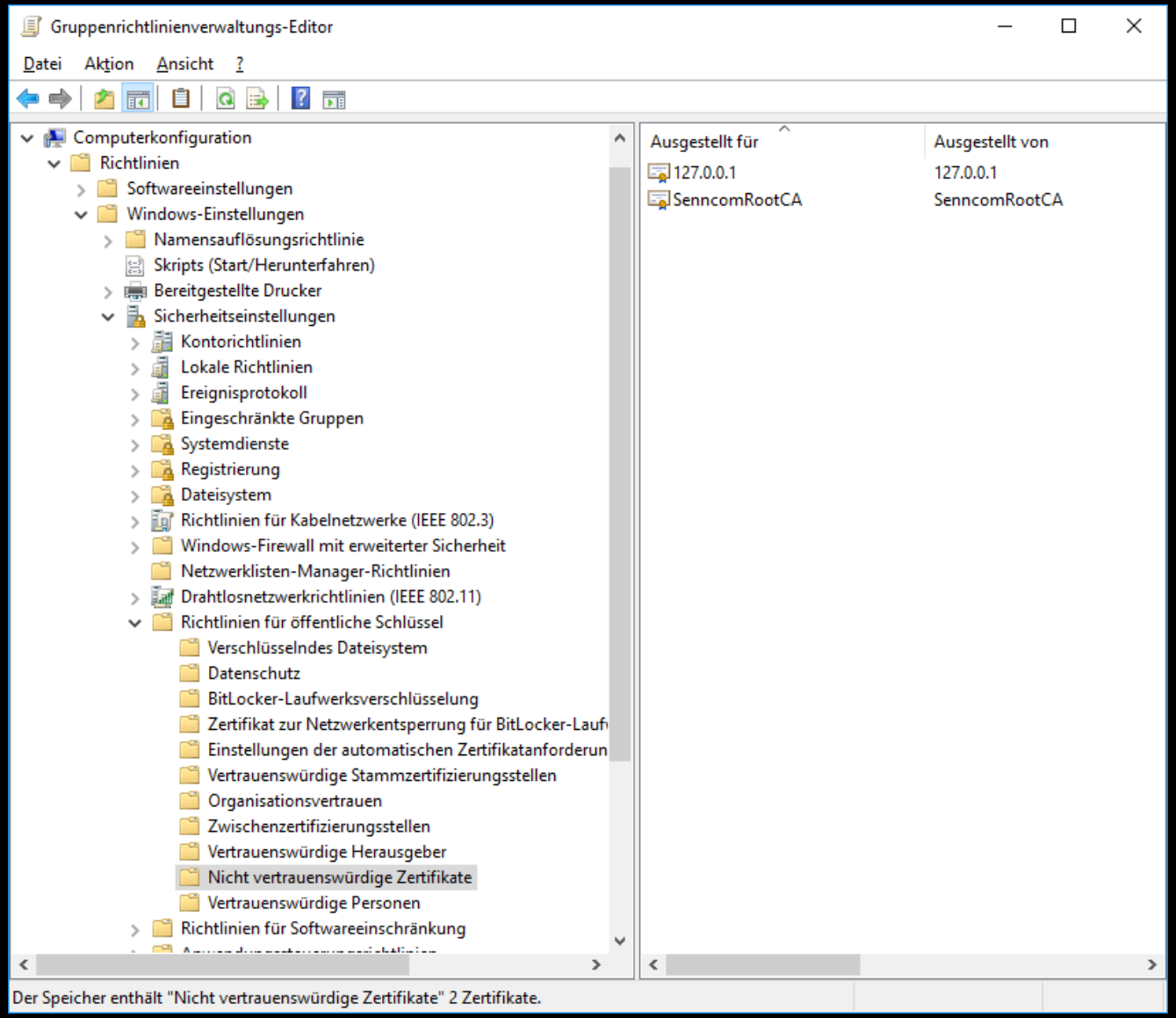
Die Realität – Stand November 2018

- Chrome (70.0.3538.77) – erlaubt
- Firefox (63.0.1) – verboten
- Internet Explorer 11 – verboten
- Edge – seit aktueller Version erlaubt
- Safari – verboten

Was kann der Anwender tun?

Anwender: Dem CA-Zertifikat nicht mehr vertrauen

- Manuell entfernen mittels (z. B. certlm.msc)
- Skript von Sennheiser: remove_senncom_certificates.bat
- CA-Zertifikat per Group Policy als nicht vertrauenswürdig klassifizieren



Prüfung auf verdächtige CA-Zertifikate

```
D:\Share\SysinternalsSuite>sigcheck.exe -tv

Sigcheck v2.70 - File version and signature viewer
Copyright (C) 2004-2018 Mark Russinovich
Sysinternals - www.sysinternals.com

Listing valid certificates not rooted to the Microsoft Certificate Trust List:

Machine\root:

   Secorvo Root CA 2022
        Cert Status:    Valid
        Valid Usage:    All
        Cert Issuer:    Secorvo Root CA 2022
        Serial Number:  48 4A 4B
        Thumbprint:     1F1ECE8B6E6CD0623D7DB0CAB42185EA2F845366
        Algorithm:      sha1RSA
        Valid from:     13:22 24.08.2010
        Valid to:       13:22 01.09.2022
```

- Sigcheck.exe → Sysinternals Suite
- Suche nach CA-Zertifikaten deren Vertrauensanker nicht in der Microsoft Certificate Trust List liegt

Wie kann man solche Schwachstellen beim Design vermeiden?

University of Virginia, Department of Computer Science
CS551: Security and Privacy on the Internet, Fall 2000

The Protection of Information in Computer Systems

JEROME H. SALTZER, SENIOR MEMBER, IEEE, AND
MICHAEL D. SCHROEDER, MEMBER, IEEE

About this paper

Manuscript received October 11, 1974; revised April 17. 1975.

Fourth ACM Symposium on Operating System Principles (October 1973).
Revised version in *Communications of the ACM* 17, 7 (July 1974).

Original web version created by Norman Hardy.

Invited Paper

Abstract

This tutorial paper explores the mechanics of protecting computer-stored information from unauthorized use or modification. It concentrates on those architectural structures--whether hardware or software--that are necessary to support information protection. The paper develops in three main sections. Section I describes desired functions, design principles, and examples of elementary protection and authentication mechanisms. Any reader familiar with computers should find the first section to be reasonably accessible. Section II requires some familiarity with descriptor-based computer architecture. It examines in depth the principles of modern protection architectures and the relation between capability systems and access control list systems, and ends with a brief analysis of protected subsystems and protected objects. The reader who is dismayed by either the prerequisites or the level of detail in the second section may wish to skip to Section III, which reviews the state of the art and current research projects and provides suggestions for further reading.

Glossary

Acht

Security Design Principles

und noch zwei weitere...

Economy Of Mechanism

Keep the design as simple and small as possible.

Economy Of Mechanism

- Das Root-Zertifikat wird installiert, weil...
- TLS-Zertifikat und Key gebraucht werden, um...
- HTTPS für den lokalen Web-Socket zu aktivieren...
- weil Browser das für Mixed-Content verlangen...
- um web-basierte Softphones zu unterstützen

- **Höchste Vorsicht bei derartiger Komplexität!**
- Browser-Hersteller:
  - Localhost nicht als Mixed Content behandeln
  - Einfacher Zugriff auf lokale Geräte?

Fail-safe Defaults

Base access decisions on permission rather than exclusion.

Fail-safe Defaults

- Nur ein Bruchteil der Anwender nutzt tatsächlich web-basierte Softphones
- Zertifikat und Key werden immer ohne Warnhinweis installiert

- WebSocket-Dienst nur auf explizite Anforderung durch den Anwender installieren

Complete Mediation

Every access to every object must be checked for authority.

Complete Mediation

- Der private Key liegt als Datei im Programmordner
- Anwendung muss selbst für den Schutz sorgen
- Verschlüsselt, aber mit leicht zu findenden Passwörtern

- Private Key im Windows Key Store (bzw. MacOS Key Chain) ablegen

Open Design

The design should not be secret.

**The mechanisms should not depend on the ignorance of potential attackers,
but rather on the possession of specific, more easily protected, keys or passwords.**

Open Design

- Für alle Installationen gleiche, fest im Code oder Konfigurationsdateien hinterlegte Passwörter bzw. Schlüssel

- Passwörter und Schlüssel bei jeder Installation neu generieren

Separation of Privilege

Where feasible, a protection mechanism that requires two keys to unlock it is more robust and flexible.

Separation of Privilege

- Es wird ein Root-Zertifikat in einem systemweiten Certificate Store installiert

- An die Adresse der Systembetreiber:
  - Benutzern die Installation von Root-Zertifikaten verbieten
  - Installationen nur per Software-Management
  - Prüfung des Verhaltens der Software im Vorfeld
  - Benutzer ohne lokale Administrationsrechte?

Least Privilege

Every program and every user should operate using the least set of privileges necessary to complete the job.

Least Privilege

- Installiert ein Root-Zertifikat, wo lediglich ein gültiges Serverzertifikat benötigt wird
- Belässt das Root-Zertifikat auch nach einer Deinstallation dort

- Nur das benötigte Server-Zertifikat lokal als vertrauenswürdig installieren, kein Root-Zertifikat
- Bei Deinstallation das Zertifikat wieder aus dem System-Store löschen

Least Common Mechanism

Minimize the amount of mechanism common to more than one user and depended on by all users

Least Common Mechanism

- Das Root-Zertifikat wird in einem systemweit für alle Anwender und Anwendungen gültigen Certificate Store installiert

- Installation in den lokalen Systemstore
  - User Certificate Store ebenfalls problematisch
- Im AD besser: Zentrale Installation per Certificate Trust List über Group Policy

Psychological Acceptability

The mechanisms must match the user's mental image of the protection goal

Psychological Acceptability

- Keinerlei Hinweis an den Anwender
- Kein Anwender vermutet, dass eine Headset-Middleware am PKI-Vertrauensmodell des Systems hantiert

- Installation nur nach expliziter Anforderung durch den Anwender, mit einschlägigen Hinweisen
- An die Adresse von Microsoft:
  - Wieso kann Third-Party Software den obligatorischen Warnhinweis unterdrücken?

Work Factor

Compare the cost of circumventing the mechanism with the resources of a potential attacker.

Work Factor

- Ein konstantes Schlüsselpaar / Zertifikat für alle Installationen

- Public-Key Schlüsselpaar bei jeder Installation zufällig neu generieren

Compromise Recording

It is sometimes suggested that mechanisms that reliably record that a compromise of information has occurred can be used in place of more elaborate mechanisms that completely prevent loss.

Compromise Recording

- Installationen werden nicht zentral registriert
- Root-Zertifikat verbleibt nach Deinstallation auf System
- Wie können betroffene Ex-Anwender erreicht werden?

- Bei Deinstallation alle Änderungen rückgängig machen

1. Public-Key Schlüsselpaar bei jeder Installation zufällig neu generieren
2. Nur das benötigte Server-Zertifikat lokal als vertrauenswürdig installieren, kein Root-Zertifikat
3. Beim Entfernen der Software auch das Zertifikat wieder aus dem System-Store löschen
4. Web-Socket mit Zertifikat und Key nur auf explizite Anforderung durch den Anwender installieren, mit einschlägigen Hinweisen
5. Private Key im Windows Key Store (bzw. MacOS Key Chain) ablegen

May the force be with you


TOP
CONSULTANT
IT-Berater
2015
secorvo
security consulting
Ettlinger Str. 12-14
76137 Karlsruhe
Telefon +49 721 255171-0
Telefax +49 721 255171-100
info@secorvo.de
www.secorvo.de

Quellenangaben

- Icons made by Freepik from www.flaticon.com
- Bilder Titelfolie, Agenda, etc.: Wolfram Sieber/Fotoskop.de
- Bild Schlussfolie (Visitenkarte): harmonicdesign/Bigstock.com
- Folie 3: https://www.secjuice.com/security-researcher-assaulted-ice-atrient/
- Folie 7: Cross origin resource sharing (CORS) and Self-Signed Certificates Explained/Sennheiser Communications
- Folie 8: Creativa Images/Bigstock.com
- Folie 15: https://www.first.org/cvss/calculator/3.0
- Folie 17: Stephen Coburn/Bigstock.com
- Folie 19: Mikaela Wiedenhoff/unsplash.com
- Folie 20: https://www.golem.de/news/root-zertifikat-sennheiser-software-hebelt-https-sicherheit-aus-1811-137603.html
- Folie 20: https://www.heise.de/security/meldung/Sennheiser-Software-spielt-Angreifern-maechtige-Werkzeuge-in-die-Haende-4217613.html
- Folie 21: https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2018-17612
- Folie 22, 23: https://en-de.sennheiser.com/headset-software-pc?uncached=1
- Folie 24: https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/ADV180029
- Folie 26: H. Zell, CC BY-SA 3.0, aus Wikipedia
- Folie 26: Sebastian Molinares/unsplash.com
- Folie 28: https://twit.tv/shows/security-now/episodes/692, https://twit.tv/shows/security-now/episodes/693
- Folie 30: https://w3c.github.io/webappsec-mixed-content/
- Folie 33: https://github.com/w3c/webappsec-mixed-content/issues/4
- Folie 34: https://github.com/w3c/webappsec-mixed-content/commit/349501cdaa4b4dc1e2a8aacb216ced58fd316165
- Folie 35: http://www.cs.virginia.edu/~evans/cs551/saltzer/
- Folien 40 – 60: http://emergentchaos.com/the-security-principles-of-saltzer-and-schroeder