

**D • A • CH Security - 27. September 2016**

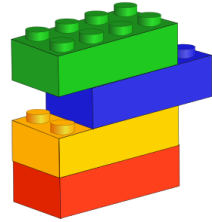
Konstantin Knorr, Hochschule Trier

Matthias Scherf, Universität Trier

Manuel Ifland, Siemens AG

# Automatisierte Erkennung bekannter Sicherheitslücken mittels CVE, CPE und NVD

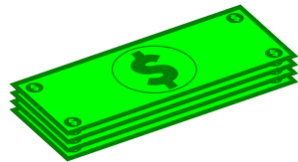
# Warum werden Softwareprodukte von Drittanbietern eingesetzt?



Fertige Bausteine



Zeitersparnis



Geringere Kosten

# Sicherheitslücken in Drittanbieterkomponenten müssen adressiert werden!

~ 50 neue gemeldete Schwachstellen täglich<sup>1</sup>

> 1000 neue/aktualisierte Softwarekomponenten täglich<sup>1</sup>

Eine von 16 Softwarekomponenten in neuester Version weisen bekannte Sicherheitslücken auf<sup>1</sup>

63% der Organisationen haben unvollständige Software Bill of Materials (BOM)<sup>1</sup>

Quelle:

<sup>1</sup> 2015 Sonatype State of the Software Supply Chain Report

Vulnerabilities By Year



Quelle: cvedetails.com

# Relevante Schwachstellen-Standards



CVE-2016-5253



cpe:/a:adobe:flash\_player:19.0.0.245



CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H



CWE-79 (Cross-Site Scripting)

# Verwendung der Standards in der National Vulnerability Database (NVD)

**Vulnerability Summary for CVE-2016-5253**

Original release date: 08/04/2016  
Last revised: 08/05/2016  
Source: US-CERT/NIST

**CVE**

**Overview**  
The Updater in Mozilla Firefox before 48.0 on Windows allows local users to write to arbitrary files via vectors involving the callback application-path parameter and a hard link.

**Impact**

<b>CVSS Severity (version 3.0):</b> CVSS v3 Base Score: <u>4.7</u> Medium Vector: <u>CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N</u> Impact Score: 3.6 Exploitability Score: 1.0	<b>CVSS Severity (version 2.0):</b> CVSS v2 Base Score: <u>4.7</u> MEDIUM Vector: <u>(AV:L/AC:M/Au:N/C:N/I:C/A:N)</u> (legend) Impact Subscore: 6.9 Exploitability Subscore: 3.4
---	--

**CVSS**

**CVSS Version 3 Metrics:**  
Attack Vector (AV): Local  
Attack Complexity (AC): High  
Privileges Required (PR): Low  
User Interaction (UI): None  
Scope (S): Unchanged  
Confidentiality (C): None  
Integrity (I): High  
Availability (A): None

**CVSS Version 2 Metrics:**  
Access Vector: Locally exploitable  
Access Complexity: Medium  
Authentication: Not required to exploit  
Impact Type: Allows unauthorized modification

**References to Advisories, Solutions, and Tools**  
By selecting these links, you will be leaving NIST webpage. We have provided these links to other web sites because they may have information that would be of interest to you, with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page.

**External Source:** CONFIRM  
Name: <http://www.mozilla.org/security/announce/2016/mfsa2016-69.html>  
Type: Vendor Advisory  
Hyperlink: <http://www.mozilla.org/security/announce/2016/mfsa2016-69.html>

**External Source:** CONFIRM  
Name: [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1246944](https://bugzilla.mozilla.org/show_bug.cgi?id=1246944)  
Type: Issue Tracking; Permissions Required  
Hyperlink: [https://bugzilla.mozilla.org/show\\_bug.cgi?id=1246944](https://bugzilla.mozilla.org/show_bug.cgi?id=1246944)

**Vulnerable software and versions**

**CPE**

**Configuration 1**  
\* OR  
\* cpe:/a:mozilla:firefox:47.0.1 and previous versions

\* Denotes Vulnerable Software  
[Changes related to vulnerability configurations](#)

**Technical Details**

**CWE**

**Vulnerability Type (View All)**  
Permissions, Privileges, and Access Control (CWE-264)  
CVE Standard Vulnerability Entry <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5253>

## CVSS Severity (version 3.0):

CVSS v3 Base Score: 4.7 Medium

Vector: CVSS:3.0/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:H/A:N

Impact Score: 3.6

Exploitability Score: 1.0

## CVSS Version 3 Metrics:

Attack Vector (AV): Local

Attack Complexity (AC): High

Privileges Required (PR): Low

User Interaction (UI): None

Scope (S): Unchanged

Confidentiality (C): None

Integrity (I): High

Availability (A): None

## Technical Details

### Vulnerability Type (View All)

Permissions, Privileges, and Access Control (CWE-264)

CVE Standard Vulnerability Entry <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-5253>

## Vulnerable software and versions

### + Configuration 1

\* OR

\* cpe:/a:mozilla:firefox:47.0.1 and previous versions

## CVSS Severity (version 2.0):

CVSS v2 Base Score: 4.7 MEDIUM

Vector: (AV:L/AC:M/Au:N/C:N/I:C/A:N) (legend)

Impact Subscore: 6.9

Exploitability Subscore: 3.4

## CVSS Version 2 Metrics:

Access Vector: Locally exploitable

Access Complexity: Medium

Authentication: Not required to exploit

Impact Type: Allows unauthorized modification

# Studie und Vorgehen

- 26 frei verfügbare, populäre Softwareprodukte (z.B. Mozilla Firefox, WinRAR, Skype, .NET-Framework, VLC Player) wurden auf Windows 7 installiert → Softwareprofil
- Untersuchungszeitraum war vom 23.08.2015 bis zum 20.11.2015
- Tägliche Prüfung nach Sicherheitslücken mittels Secunia PSI (heute Flexera PSI)
- Ex-post Auswertung der NVD-Datenbank mittels des selbst entwickelten Tools „Software Vulnerability Tool“ (SVT)
- SVT wurde in C# und .NET entwickelt und verwendet SQLite. Download unter <http://public.hochschule-trier.de/~knorr/DACH2016>
- Vergleich der SVT und Secunia PSI-Ergebnisse

# „Software Vulnerability Tool“ (SVT)

Software-Vulnerability-Tool

CWE-Statistik

Anzahl Einträge in DB: letzte Datenbankaktualisierung: 2.6.2016

CVE	76156	CVSS	76137
CPE	208976	CWE	43785

Suche

‘CVE-‘

Produktbezeichnung:

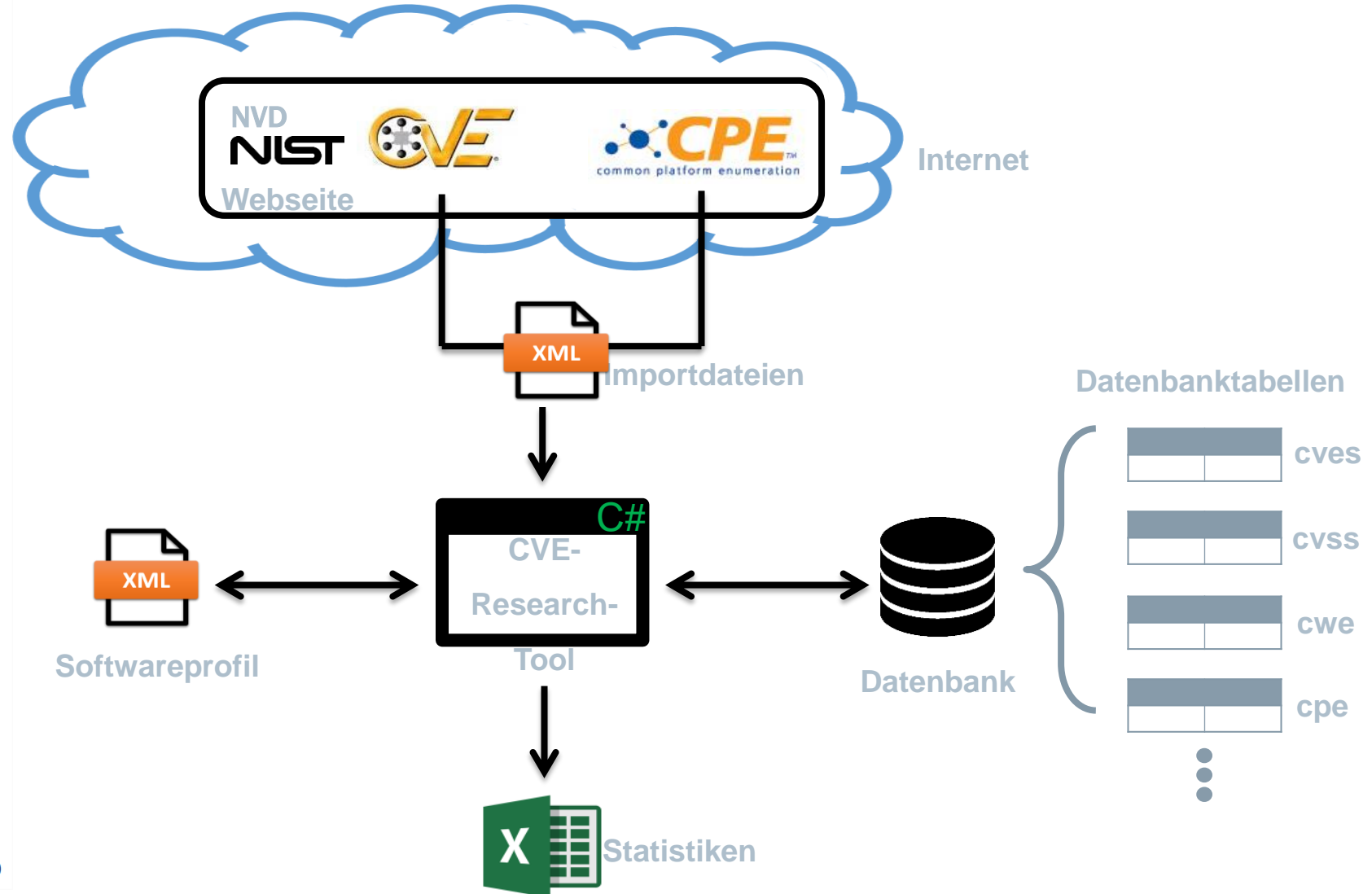
Zeitraum von: 01.05.2016 bis: 02.06.2016

1080 CVE-Einträge gefunden

CVE-Id	erstellt am	aktualisiert
CVE-2015-0116	29.06.2015, 00:59:02	26.05.2016, 14:24:11
CVE-2015-0569	09.05.2016, 12:59:00	10.05.2016, 00:01:34
CVE-2015-0570	09.05.2016, 12:59:01	10.05.2016, 17:00:13
CVE-2015-0571	09.05.2016, 12:59:02	10.05.2016, 17:09:24
CVE-2015-0857	06.05.2016, 19:59:00	09.05.2016, 21:26:59
CVE-2015-0858	06.05.2016, 19:59:01	09.05.2016, 20:36:34
CVE-2015-1322	29.04.2015, 22:59:01	26.05.2016, 15:48:48
CVE-2015-1350	02.05.2016, 12:59:07	06.05.2016, 18:55:03
CVE-2015-1498	16.02.2015, 16:59:11	19.05.2016, 00:36:31
CVE-2015-1547	13.04.2016, 19:59:01	18.05.2016, 23:45:52
CVE-2015-1573	02.05.2016, 12:59:08	06.05.2016, 16:49:34

HOCHSCHULE TRIER  
Trier University of Applied Sciences  
Informatik - Computer Science

Version 1.0  
von Matthias Scherf (scherf@outlook.com)



# Ergebnisse für das Softwareprofil (aka BOM)

- 10 von 26 Produkten hatten Sicherheitslücken
- 286 CVE-Nummern, Spitzenreiter: Apple iTunes (75), Adobe Acrobat Reader (58), Adobe Flash Player (50)
- Unterschiedliche Gegenmaßnahmen: Neue Version vs. Patch (bei Win7)
- $6,8 \leq \text{CVSS-Base-Score} \leq 9,2$
- Nur zehn CWE-IDs, Spitzenreiter CWE-119 (“Improper Restriction of Operations within the Bounds of a Memory Buffer”)
- 81 CVEs hatten keine CWE-ID zugewiesen



# Vergleich SVT mit Secunia PSI

Softwareanwendung	Sicherheitslücken gefunden von	
	Secunia PSI	Software Vulnerability Tool
.NET Framework	Ja	zu ungenaue Versionsangabe in CPE
7-Zip	Nein	Nein
Adobe Flash Player	Problem durch Update auf neue Version	Ja
Adobe Reader	Ja	Ja
AdwCleaner	Nein	Nein
Apache OpenOffice	Ja	Ja
Apple iTunes	Angabe fragwürdiger CVEs	Ja
Ccleaner	Nein	Nein
CDBurnerXP	Nein	Nein
FileZilla	Nein	Nein
Gimp	Nein	Nein
Google Chrome	Problem durch Update auf neuere Version	Ja
	Angabe fragwürdiger CVEs	
IrfanView	Nein	Nein
Java Runtime Environment	Angabe fragwürdiger CVEs	Ja
KMPlayer	Nein	Nein
Microsoft Internet Explorer	Ja	zu ungenaue Versionsangabe in CPE
Microsoft Silverlight	Nein	Nein
Mozilla Firefox	Problem durch Update auf neuere Version	Ja
Notepad++	Nein	Nein
PDFCreator	Nein	Nein
Putty	Angabe fragwürdiger CVE	Nein
Recuva	Nein	Nein
Skype	Nein	Nein
TrueCrypt	Nein	Nein
VLC Player	Nein	Ja
Windows 7	Ja	Ja
WinRAR	Nein	Nein

# Diskussion

- Gutes Zusammenspiel zwischen CVE und CVSS: fast 100% CVEs haben CVSS-Score (nur Base Score)
- CWE-CVE-Zusammenspiel schlecht: Nur 57% der CVEs haben CWE, nur 29 CWE-IDs werden verwendet
- Probleme bei CPE:
  - Neue CVE-Einträgen häufig ohne CPE
  - Fehlende bzw. ungenaue CPE-Zuordnungen: Nur die aktuellste Softwareversion wird in CPE angegeben
  - Detaillierungsgrad bei CPE oft nicht genau genug.  
Bsp.: Version 4.5.50709 vs. CPE-Version 4.5 für das .NET-Framework
  - Problem der automatisierten CPE-Generierung mit Onboard-Mitteln
- Unterschiedliche Versionen der Standards: CVSS v2 vs. v3, NVD XML-Schema v2.0 vs. v2.1

# Fazit

- CVE / NVD größte und am stärksten eingesetzte frei-verfügbare Schwachstellen-Datenbank
- Gutes Zusammenspiel zwischen CVE und CVSS
- CVSS erlaubt detaillierte Entscheidung pro Sicherheitslücke
- CPE-Zuordnung teilweise zu ungenau oder nicht vorhanden
- Unterstützung von CPE durch Software-Hersteller ausbaufähig
- CWE-Verwendung überschaubar
- Patch-orientierter Ansatz mit CVE-Datenbank nur bedingt möglich

# Ein Blick in die Zukunft

- Zunehmende Kommerzialisierung von Sicherheitslücken
- Sammeln / Verkauf von Exploits
- Abkehr vom klassischen Responsible-Disclosure hin zum Non-Disclosure-Paradigma
- Verringerung der Anzahl kostenfreier Datenbanken für Sicherheitslücken
- Größeres Angebot an kommerziellen Schwachstellen-Datenbanken
- Vermehrt Bug Bounty Programme



# Kontakt

## **Prof. Dr. Konstantin Knorr**

Fachbereich Informatik

Hochschule Trier

Am Schneidershof, F201

Postfach 1826

D-54208 Trier

E-Mail: [knorr@hochschule-trier.de](mailto:knorr@hochschule-trier.de)

## **Manuel Ifland, CISSP**

Siemens ProductCERT

Siemens AG

Corporate Technology

Otto-Hahn-Ring 6

D-81739 München

E-Mail: [manuel.ifland@siemens.com](mailto:manuel.ifland@siemens.com)

# Backup-Folien

# Ergebnisse

## Globale Ergebnisse mittels SVT

- 72.903 CVE-Einträge importiert
- 41.239 hatten eine Verknüpfung mit einer CWE-ID
- 1.921.344 CVE-CPE-Verknüpfungen
- CPEs: 87% Anwendungen, 8% Betriebssysteme, 5% Hardware
- Nur CVSS-Base-Score enthalten
- CVSS-Mittelwert bei 7,5
- 5.293 CVEs haben CVSS-Score 10.0
- Nur 29 von mehreren Tausend möglichen CWE-IDs werden verwendet
- CWE-79 (Cross-Site Scripting) Spitzenreiter

## Ergebnisse für das Softwareprofil

- 10 von 26 Produkten hatten Sicherheitslücken.
- 286 CVE-Nummern, Spitzenreiter: Apple iTunes (75), Adobe Acrobat Reader (58), Adobe Flash Player (50)
- Unterschiedliche Gegenmaßnahmen: Neue Version vs. Patche (bei Win7)
- $6,8 \leq \text{CVSS-Base-Score} \leq 9,2$
- Nur zehn CWE-IDs, Spitzenreiter CWE-119 (Improper Restriction of Operations within the Bounds of a Memory Buffer)
- 81 CVEs hatten keine CWE-ID zugewiesen.



# Patch Management Process for Industrial Control Systems

