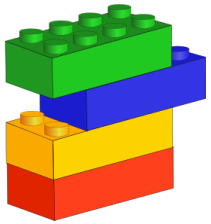
FreeImages.com/Sigurd Decroos.

D • A • CH Security - 27. September 2016

Konstantin Knorr, Hochschule Trier
Matthias Scherf, Universität Trier
Manuel Ifland, Siemens AG

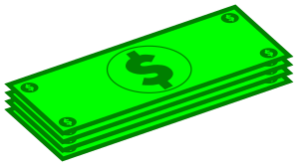
Automatisierte Erkennung bekannter Sicherheitslücken mittels CVE, CPE und NVD

Warum werden Softwareprodukte von Drittanbietern eingesetzt?



Fertige Bausteine

Zeitersparnis



Geringere Kosten

Sicherheitslücken in Drittanbieterkomponenten müssen adressiert werden!

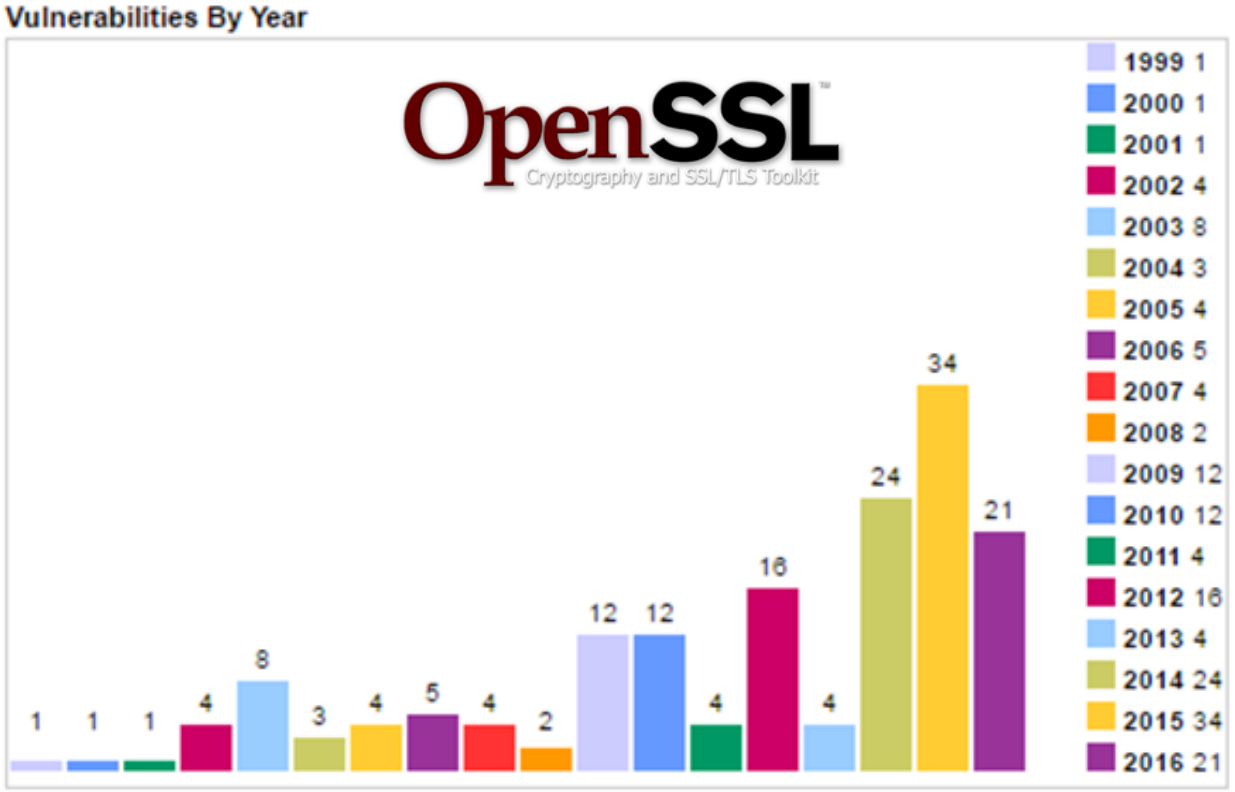
~ 50 neue gemeldete Schwachstellen täglich[1]

> 1000 neue/aktualisierte Softwarekomponenten täglich[1]

Eine von 16 Softwarekomponenten in neuester Version weisen bekannte Sicherheitslücken auf[1]

63% der Organisationen haben unvollständige Software Bill of Materials (BOM)[1]

Quelle:
[1] 2015 Sonatype State of the Software Supply Chain Report



Quelle: cvedetails.com

Relevante Schwachstellen-Standards

Common Vulnerabilities and Exposures (CVE)

Identifier

CVE-2016-5253

Common Vulnerability Scoring System (CVSS)

Kritikalität

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

Common Platform Enumeration (CPE)

Betroffene SW

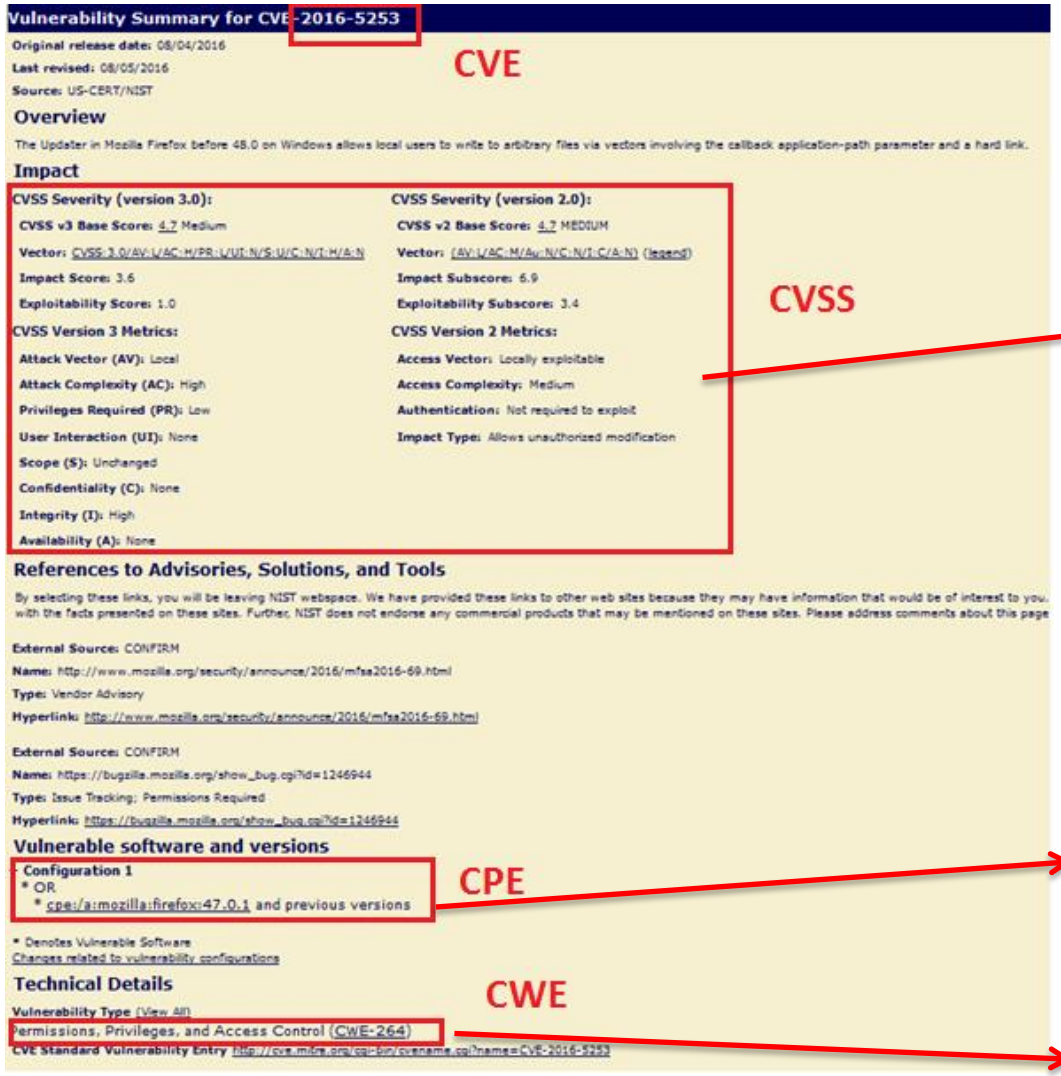
cpe:/a:adobe:flash_player:19.0.0.245

Common Weakness Enumeration (CWE)

Ursache der Schwachstelle

CWE-79 (Cross-Site Scripting)

Verwendung der Standards in der National Vulnerability Database (NVD)



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

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

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

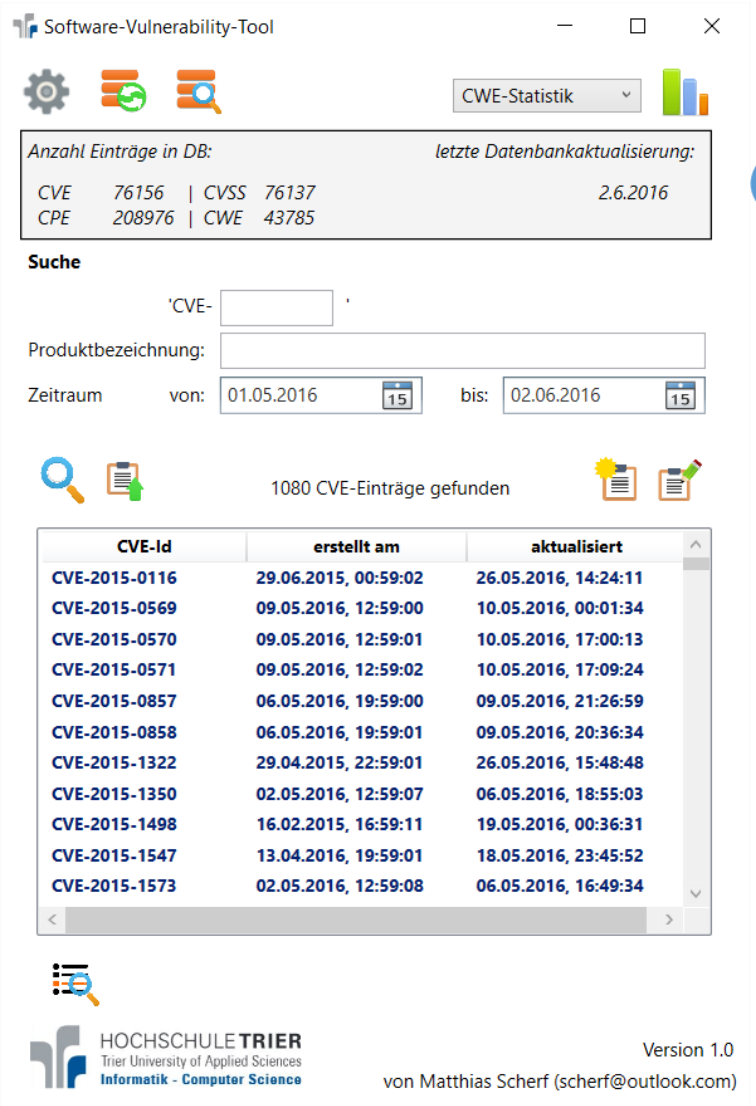
* OR

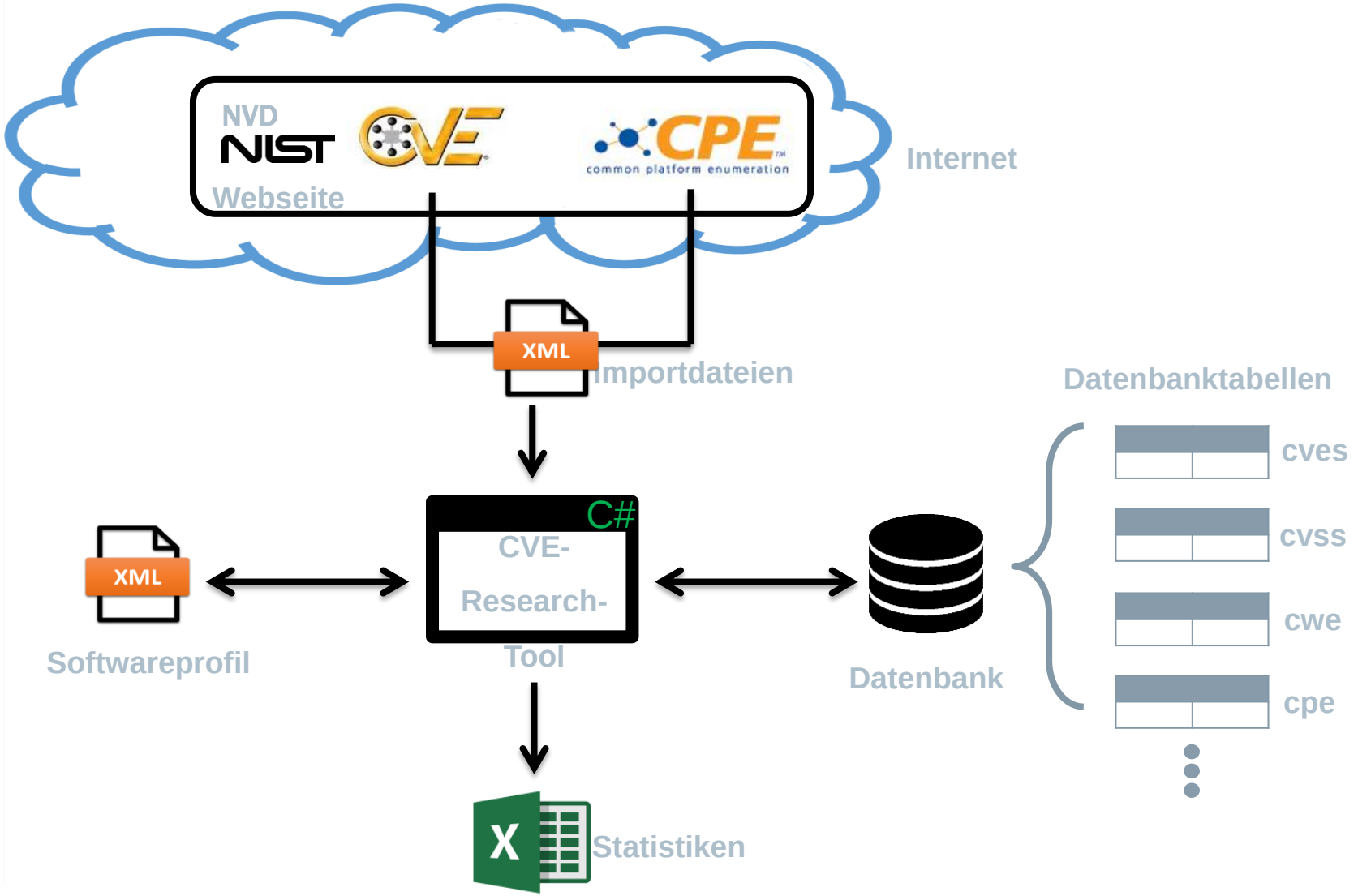
* cpe:/a:mozilla:firefox:47.0.1 and previous versions

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)





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 ≤ CVSS-Base-Score ≤ 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

	Sicherheitslücken gefunden von	
Softwareanwendung	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 Angabe fragwürdiger CVEs	Ja
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-Disclusure-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

Manuel Ifland, CISSP
Siemens ProductCERT
Siemens AG
Corporate Technology
Otto-Hahn-Ring 6
D-81739 München
E-Mail: manuel.ifland@siemens.com

SIEMENS

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 ≤ CVSS-Base-Score ≤ 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