Hochschule Hof
University of Applied Sciences

Hochschule Hof
IT-Sicherheit
Wintersemester 2025/2026

# Studienarbeit über die Schwachstelle

# CVE-2016-5195

Frederik Schwarz(000000) Lars- Johan Schrenk(0000000)

18 Dec 2025

**Abstract**

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos.

# Inhaltsverzeichnis

# Abkürzungen

**COW**. Copy-on-Write. is a resource management technique used in container storage. It allows multiple containers to share the same base filesystem layers, only copying data when modifications are made. CoW significantly reduces storage usage and improves container startup times. 5

**CVE**. Common Vulnerabilities and Exposures. is a system that provides a standardized method for identifying and cataloging publicly known cybersecurity vulnerabilities in software and hardware. Each vulnerability is assigned a unique identifier, known as a CVE ID, which helps organizations communicate and manage security issues effectively. 5

# 1. Einführung

## 1.1. Was ist der Linux kernel

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

## 1.2. Wo wird Linux(kernel) verwendet

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

## 1.3. Was ist Dirty COW

CVE −2016-5195 oder auch bekannt als "Dirty COW", ist eine kritische Sicherheitslücke im Linux-Kernel, die 2016 entdeckt wurde. Die Lücke ermöglicht es einem angreifenden Benutzer, schreibbare Bereiche des Systems zu manipulieren, ohne über die notwendigen Berechtigungen zu verfügen. Der Name "Dirty COW" und das Logo(Copy-on-Write (COW)) leitet sich von der Funktionsweise des Copy-on-Write (COW) Mechanismus ab, bzw von einer Schwachstelle COW Speichersystems.


Abbildung 1: Dirty COW Logo

Bei der Ausnutzung dieser Schwachstelle kommt es zu einer Race Condition im COW Machanismus des Kernels, wodurch ein Angreifer eine schreibbare Referenz auf eigentlich schreibgeschützte, private Speicherbereiche erhält bevor COW erfolgreich ausgeführt werden konnte. Praktisch bedeutet das Angreifer ihre Berechtigungen auf dem System erhöhen können um sich z.B. Root-Zugriff zu verschaffen.

Die Schwachstelle wurde von Phil Oester entdeckt und im gleichen Jahr behoben, jedoch wurde dieser Patch im Jahr 2017 rückgängig gemacht, da der Patch eine neue Sicherheitslücke im Kernel verursachte. [1], [2]

## 1.4. Wie weit verbreitet war/ist die Schwachstelle

Dirty COW war eine äußerst kritische Schwachstelle im Linux-Kernel die über einen langen Zeitraum unentdeckt blieb. Die Schwachstelle bestand bereits in Version 2.6.22 und wurde erst in Version 4.8.3 gepatched. Dies betraf sowohl Desktop, Server als auch Android Geräte. Da dies ein Kernel Bug war betraf dies alle Linux Distributione von 2007 bis 2016. Unter anderem wurde der Exploit in the wild zum rooten von Android Geräten verwendet. [1], [2], [3]

Diese Schwachstelle war somit nicht nur theoretisch sondern wurde auch in der Praxis exlpoitet, war für lange Zeit verbreitet und hat alle Linux basierten Geräte betroffen. Somit kan man sagen das dies eine der wichtigsten Schwachstellen im Linux-Kernel war.

Um die Tragweite dieser Problematik zu illustrieren, lassen sich mehrere statistische Kennzahlen heranziehen. Weltweit lag der Marktanteil von Android im Jahr 2017 bei etwa 72% [4], was einer Verbreitung auf schätzungsweise 1,7 bis 2 Milliarden Endgeräten entspricht.Darüber hinaus zeigen aktuelle Erhebungen, dass 96,3 % der eine Million meistfrequentierten Webserver auf Linux-basierte Systeme setzen und sämtliche der 500 leistungsstärksten Supercomputer mit Linux betrieben

werden [5]. Diese Werte verdeutlichen, dass die betreffende Schwachstelle nicht nur eine enorme Anzahl von Endgeräten betraf, sondern zugleich einen erheblichen Teil der globalen IT Infrastruktur. Zu beachten ist, dass die zugrunde liegenden Daten der Server Usage aus dem Jahr 2025 stammen und somit in Bezug auf den Zeitraum 2016/2017 potenziell geringfügige Abweichungen aufweisen können.

### 1.5. Warum ist das relevant / warum sollte man es lesen?

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

## 2. Hintergrund

### 2.1. Privilegieneskalation

Privilegieneskalation bezeichnet den Vorgang, bei dem ein Angreifer unberechtigterweise höhere Zugriffsrechte innerhalb eines Systems erlangt. Der Prozess beginnt typischerweise mit der Kompromittierung eines initialen, eingeschränkten Kontos, etwa durch Phishing, den Einsatz von Schadsoftware oder das Erraten von Zugangsdaten. Auf dieser Grundlage verfolgt der Angreifer das Ziel, seine Berechtigungen schrittweise bis hin zu administrativen bzw. Root Rechten auszuweiten [6].

Die lokale Privilegieneskalation beschreibt Szenarien, in denen ein Angreifer bereits einen begrenzten Zugriff auf ein Endgerät besitzt und vorhandene Schwachstellen im Betriebssystem oder in lokal ausgeführten Diensten ausnutzt, um seine Rechte weiter zu erhöhen. Ein solcher lokaler Zugriff kann beispielsweise durch die Ausführung von Schadsoftware, durch erfolgreiche Code-Injection-Angriffe(Webserver Exploit) oder anderen lokal betriebenen Anwendungen erreicht werden.

## 2.2. Linux File Permission

## 2.3. Linux kernel

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

## 2.4. Race-Condition

Eine Race Condition tritt auf, wenn mehrere Threads oder Prozesse gleichzeitig auf dieselbe Ressource zugreifen und dieser Zugriff nicht hinreichend synchronisiert wird. Dies kann zu nichtdeterministischen Ergebnissen, fehlerhaften Systemzuständen oder sogar zu Datenkorruption führen. Eine notwendige Bedingung für das Auftreten einer Race Condition ist, dass mindestens ein beteiligter Zugriff schreibend erfolgt und gleichzeitig ein weiterer Zugriff(sei er lesend oder schreibend) stattfindet. Unter diesen Voraussetzungen können sich die einzelnen Operationen überlappen und unbeabsichtigte Wechselwirkungen hervorrufen.

Ursächlich für solche Probleme ist meist die fehlende Atomarität der ausgeführten Operationen.

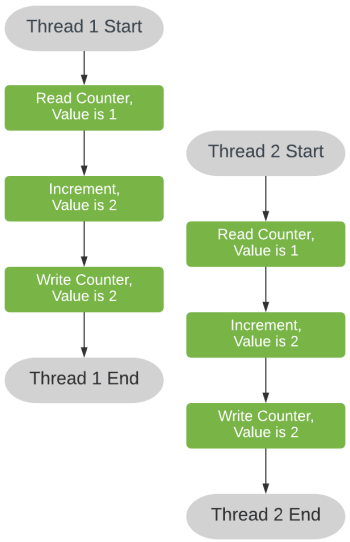


Abbildung 2: Race Condition: Increment

Wie in Abbildung 2 dargestellt, werden zwei Threads gestartet, die eine gemeinsame Variable modifizieren. Die Operation increment ist nicht atomar. Sie besteht vielmehr aus einer Sequenz von read, increment und write. Erfolgt das read des zweiten Threads, bevor der erste Thread den neuen Wert nach Abschluss seiner Operation zurückschreiben kann, lesen beide Threads denselben Anfangswert und berechnen dieselbe Aktualisierung. Dadurch wird die Variable zwar zweimal verändert, jedoch auf denselben Endwert gesetzt. Dies ist ein klassischer Fall einer verlorenen Aktualisierung (lost update).

Neben verlorenen Updates existieren weitere Kategorien von Race Conditions. Ein häufiges Szenario ist das Time-of-Check to Time-of-Use-Problem (TOCTOU), bei dem sich ein Systemzustand zwischen einer Überprüfung und einer anschließenden Verwendung unbemerkt ändert. Ebenfalls verbreitet, insbesondere in Sprachen wie C und C++, sind Use-After-Free Races. Hierbei wird bereits freigegebener Speicher weiterverwendet, während das Programm fälschlicherweise davon ausgeht, dass dieser Speicherbereich weiterhin gültig sei. Dies ermöglicht es anderen Prozessen oder Threads, denselben Speicher zwischenzeitlich neu zu belegen, was zu gravierenden Fehlfunktionen oder Sicherheitslücken führen kann.[7]

# 3. CVE-2016-5195: Dirty COW

## 3.1. Details der Schwachstelle

### 3.1.1. Summary

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

### 3.1.2. Technische Ursache

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri

amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

#### 3.1.3. Ursprung/code beispiel

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

### 3.2. Ausnutzen der Schwachstelle

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opinemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

### 3.3. Verteidigung

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim aeque doleamus animo, cum corpore dolemus, fieri tamen permagna accessio potest, si aliquod aeternum et infinitum impendere malum nobis opi-

nemur. Quod idem licet transferre in voluptatem, ut postea variari voluptas distinguique possit, augeri amplificarique non possit. At etiam Athenis, ut e patre audiebam facete et urbane Stoicos irridente, statua est in quo a nobis philosophia defensa et collaudata est, cum id, quod maxime placeat, facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet, ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum defuturum, quas natura non depravata desiderat. Et quem ad me accedis, saluto: 'chaere,' inquam, 'Tite!' lictores, turma omnis chorusque: 'chaere, Tite!' hinc hostis mi Albucius, hinc inimicus. Sed iure Mucius.

## 4. Verwandte Arbeiten

## 5. Fazit

## Literatur


[1] D. C. Inc., „Dirty COW (CVE-2016-5195) HomePage“. Zugegriffen: 18. November 2025. [Online]. Verfügbar unter: https://dirtycow.ninja/

[2] I. Anuradha, „Dirty COW (Privilege Escalation)“, S. , 2020.

[3] D. GOODIN, „Android phones rooted by “most serious” Linux escalation bug ever“. Zugegriffen: 18. November 2025. [Online]. Verfügbar unter: https://arstechnica.com/information-technology/2016/10/android-phones-rooted-by-most-serious-linux-escalation-bug-ever/

[4] N. Kumar, „Android Usage Statistics (2025) – Users & Market Share“. Zugegriffen: 8. Dezember 2025. [Online]. Verfügbar unter: https://www.demandsage.com/android-statistics/

[5] R. Saive, „Why Linux Powers Everything From Your Coffee Machine to Mars Rovers“. Zugegriffen: 8. Dezember 2025. [Online]. Verfügbar unter: https://www.tecmint.com/why-the-world-runs-on-linux/

[6] B. Lenaerts-Bergmans, „WHAT IS PRIVILEGE ESCALATION?“. Zugegriffen: 18. November 2025. [Online]. Verfügbar unter: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/privilege-escalation/

[7] baeldung, „What Is a Race Condition?“. Zugegriffen: 18. November 2025. [Online]. Verfügbar unter: https://www.baeldung.com/cs/race-conditions