

Oops das wird teuer

Epische Fails in der Geschichte der Software Entwicklung

→ jasie.de/security-fails

→ @jasie@machteburch.social



Bildquelle: Pirates of the Caribbean / imgflip.com

—
Vor
langer,
langer
Zeit...

Quelle:
thepeakmagazine.com.sg



Könnt ihr's
erraten?





- Datenleck März 2025
- über 1 Mio Nutzer betroffen
- entgangene Einnahmen
~250.000€ pro Tag je Casino



Bildquelle: reddit.com / deleted user



```
https://api-tma1-prd.themill.tech  
//pay/launch/payment_iq  
?localeCode=en  
&sessionId=abc  
&type=WITHDRAWAL  
&userId={userID}
```



GraphQL

"Man hat sich einen Dreck um die Sicherheit der Daten der Spieler geschert"



Die "Krawall-Influencerin" (Selbstbezeichnung) Lilith Wittmann hat wieder einmal gravierende Sicherheitslücken aufgedeckt. (Bild: privat)

19.03.2025, 21:01 Uhr Lesezeit: 11 Min.

Bildquelle: heise.de



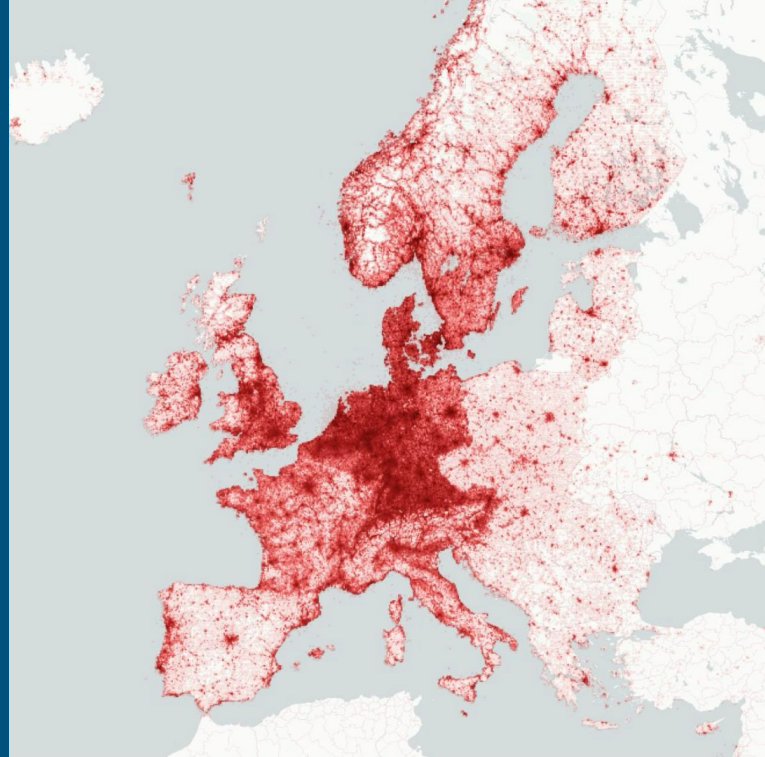
- Datenleck Dez 2024
- ca. 460.000 E-Auto-Fahrer betroffen
- pot. 13 Mrd. € Schaden



Bildquelle: memecrunch.com



Bildquelle: Thomas Starck / Auto Bild / ullstein bild



Bildquelle: CCC



- Systemausfall 12. Juli 2024
(ein Freitag... 🦴)
- ca. 8.5 Mio. Windows Rechner
betroffen
- ca. 5 Mrd. € Schaden +++





THE SOURCE OF (ABSOLUTE) TRUTH!

example: CrowdStrike


on MSN

Microsoft crash sparks chaos
at Bangkok airport

Global tech outage impacting businesses
across the country

[Microsoft is believed to be the starting point] of a global tech outage
that has impacted businesses from banks to newsrooms.

❌ Claim: A Microsoft bug

❌ Claim: A NULL-ptr dereference
... (re)tweeted over 25K times! 

✅ Fact: OOB read in CS's driver

When received by the sensor and loaded into the Content Interpreter,
problematic content in Channel File 291 resulted in an out-of-bounds memory
read triggering an exception. This unexpected exception could not be gracefully
handled, resulting in a Windows operating system crash (BSOD).

confirmed by
CrowdStrike & Microsoft

Our observations confirm CrowdStrike's analysis that this was a read-out-of-
bounds memory safety error in the CrowdStrike developed CSagent.sys driver.

Incorrect analysis



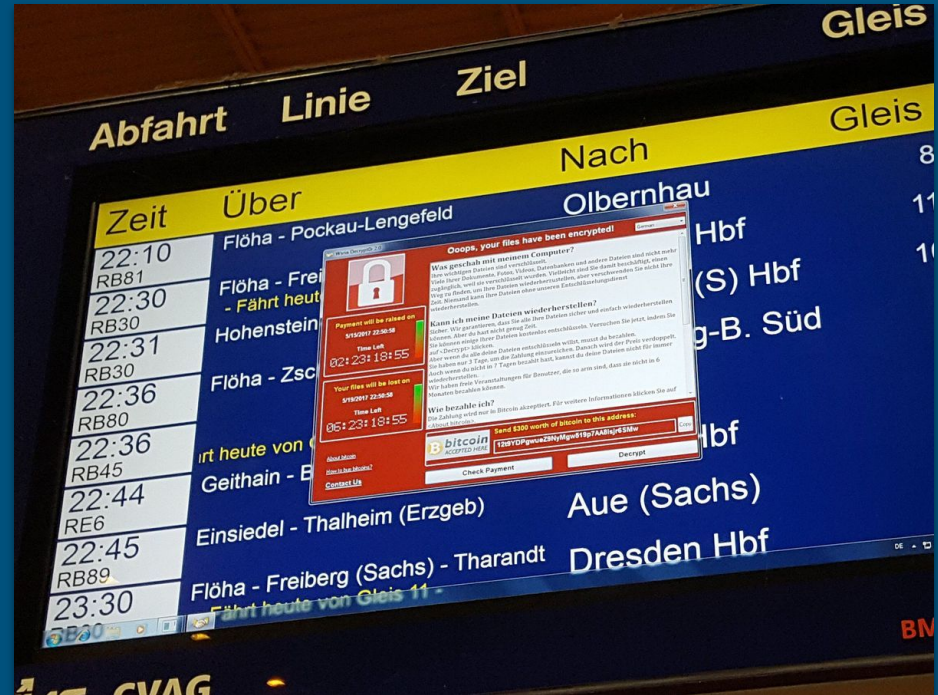
Bildquelle: Wikipedia / Smishra1

Bildquelle: objective-see.org



Wanna Cry

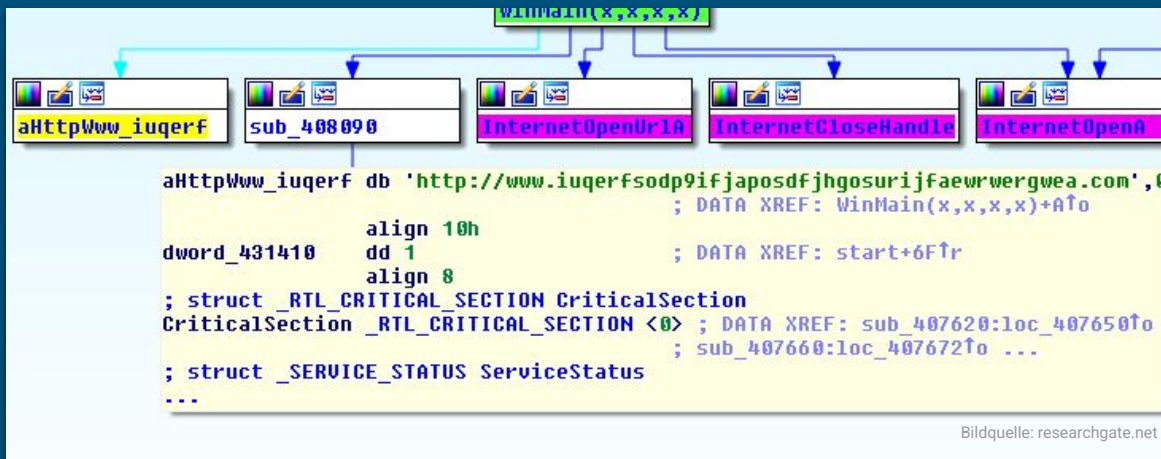
- Software-Ausfall Mai 2017
- einige Hacker betroffen 😊
- entgangene Einnahmen pot. in Millionenhöhe



Bildquelle: spiegel.de



Bildquelle: thehackernews.com



Bildquelle: researchgate.net



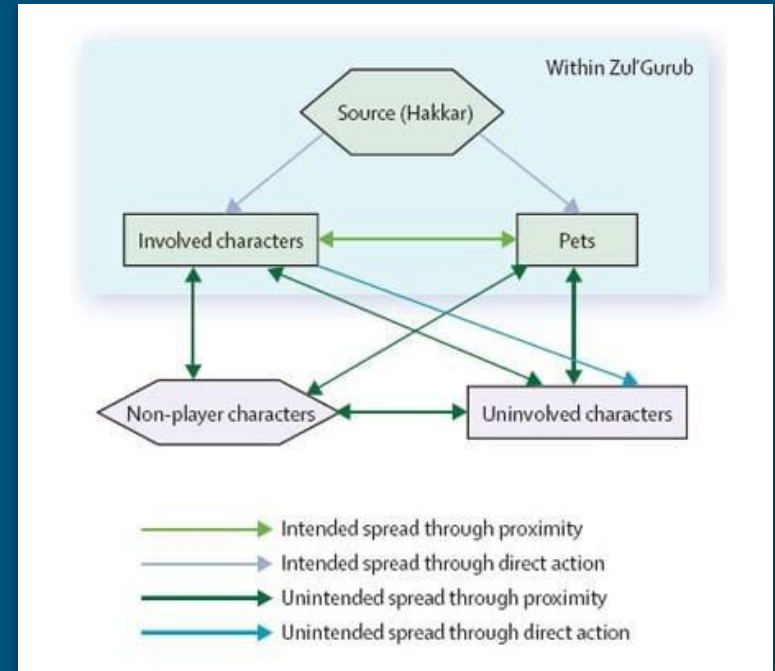
- ❑ Software-Fehler in Sep & Okt 2005
- ❑ zw. 250.000 und 500.000 MMORPG-Spieler weltweit betroffen
- ❑ Schadenshöhe 💰!



Bildquelle: reddit.com / lucaswow



Bildquelle: reddit.com / Flimsy_Card8028



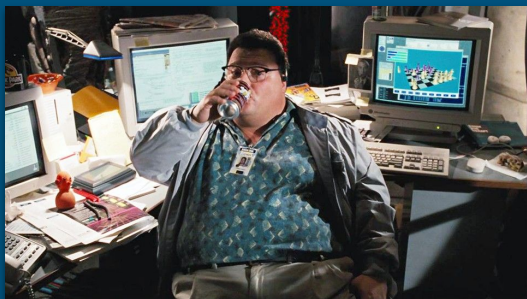
Bildquelle: blogs.cornell.edu

Fazit

✂ Secure Coding Principles

✂ Code Reviews

✂ Negative Testing



Bildquelle: Jurassic Park



→ jasie.de/security-fails

Weiterführend /1

- [1] zu Merkur Bets:
Medium: **Casinonutzer der Merkur-Gruppe verlieren nicht nur ihr Geld sondern auch ihre Daten** (2025)
lilithwittmann.medium.com/casinonutzer-der-merkur-gruppe-verlieren-nicht-nur-ihr-geld-sondern-auch-ihre-daten-ef6710184f7c
- [2] zu Merkur Bets:
heise online: **Man hat sich einen Dreck um die Sicherheit der Daten der Spieler geschert** (2025)
heise.de/hintergrund/Man-hat-sich-einen-Dreck-um-die-Sicherheit-der-Daten-der-Spieler-geschert-10321798.html
- [3] zu Volkswagen:
CCC: **Wir wissen wo dein Auto steht** (2024)
media.ccc.de/v/38c3-wir-wissen-wo-dein-auto-steht-volksdaten-von-volkswagen
- [4] zu Volkswagen:
heise online: **38C3: Terabyte an Bewegungsdaten von VW-Elektroautos in der Cloud gefunden** (2024)
heise.de/news/In-der-Cloud-abgelegt-Terabyte-an-Bewegungsdaten-von-VW-Elektroautos-gefunden-10220623.html

Weiterführend /2

- [5] zu CrowdStrike:
heise online: **Weltweiter IT-Ausfall: Betrieb wird wieder aufgenommen** (2024)
heise.de/news/Weltweiter-IT-Ausfall-Flughaefen-Banken-und-Geschaefte-betroffen-9806343.html

- [6] zu CrowdStrike:
heise online: **CrowdStrike veröffentlicht Untersuchungsbericht und bleibt Antworten schuldig** (2024)
heise.de/news/CrowdStrike-veroeffentlicht-Untersuchungsbericht-und-bleibt-Antworten-schuldig-9811796.html

- [7] zu WannaCry:
heise online: **WannaCry: Was wir bisher über die Ransomware-Attacke wissen** (2017)
heise.de/news/WannaCry-Was-wir-bisher-ueber-die-Ransomware-Attacke-wissen-3713502.html

- [8] zu WannaCry:
heise online: **Ransomware WannaCry: Sicherheitsexperte findet "Kill-Switch" – durch Zufall** (2017)
heise.de/news/Ransomware-WannaCry-Sicherheitsexperte-findet-Kill-Switch-durch-Zufall-3713420.html

Weiterführend /3

- [9] zu WoW Blutseuche:
WarCraft Wiki: **Corrupted Blood (debuff)**
[warcraft.wiki.gg/wiki/Corrupted_Blood_\(debuff\)](https://warcraft.wiki.gg/wiki/Corrupted_Blood_(debuff))

- [10] zu WoW Blutseuche:
buffed: **WoW: Wie die Zul'Gurub-Seuche von 2005 Ärzten im Kampf gegen Corona hilft** (2020)
buffed.de/World-of-Warcraft-Spiel-42971/Specials/Zul-Gurub-Seuche-Corona-1345535/

- [11] zu Secure Coding:
OWASP: **Secure Coding Practices**
owasp.org/www-project-secure-coding-practices-quick-reference-guide/stable-en/02-checklist/05-checklist

- [12] zu Negative Testing:
GeeksForGeeks: **Negative Testing in Software Engineering** (2025)
geeksforgeeks.org/negative-testing-in-software-engineering/