

## Vulnerabilità

---



Massimo Carnevali

---

Il materiale di questo corso è distribuito con licenza Creative Commons 4.0 Internazionale: Attribuzione-Condividi allo stesso modo.

<https://creativecommons.org/licenses/by-sa/4.0/>

Dove note sono state citate le fonti delle immagini utilizzate, per le immagini di cui non si è riusciti a risalire alla fonte sono a disposizione per ogni segnalazione e regolarizzazione del caso.

Massimo Carnevali

[posta@massimocarnevali.com](mailto:posta@massimocarnevali.com)

<https://it.linkedin.com/in/massimocarnevali>

"Master lock with root password" di Scott Schiller - Flickr: Master lock, "r00t" password. Con licenza CC BY 2.0 tramite Wikimedia Commons

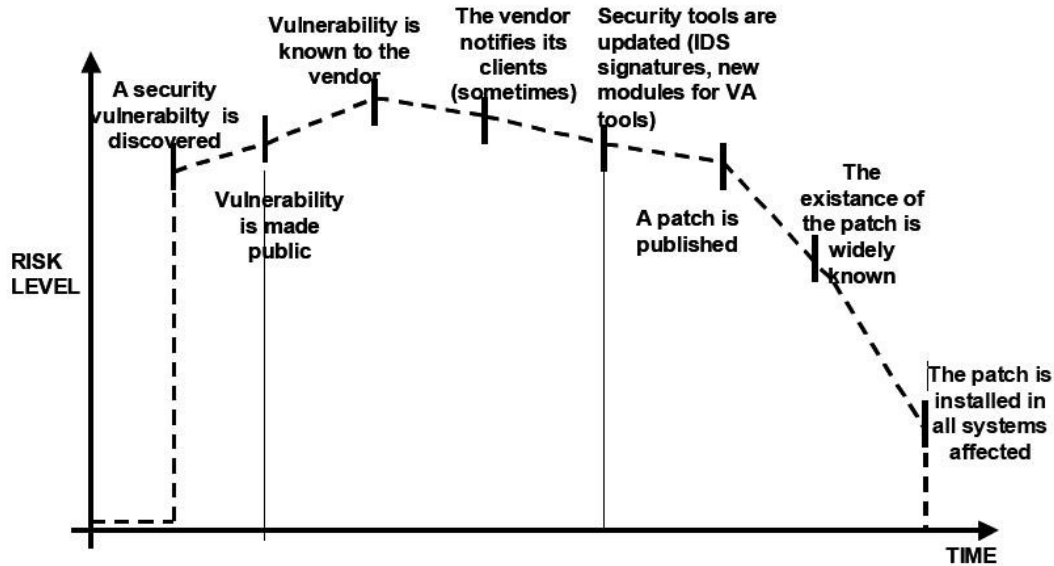
# Vulnerabilità

---

- Il concetto di vulnerabilità e il suo ciclo di vita

..

# Vulnerabilità



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

3

Full disclosure come filosofia (dibattito)

[https://en.wikipedia.org/wiki/Full\\_disclosure\\_\(computer\\_security\)](https://en.wikipedia.org/wiki/Full_disclosure_(computer_security))

Parziale (ne parlo prima con il vendor) o totale (tutto subito). Pro e contro.

Patching è un costo esterno senza nessun valore per il produttore

(tipo inquinamento, mi debbono "costringere" a mettere i filtri per non inquinare).

Fonte: OWASP

[https://www.owasp.org/index.php/Testing\\_Guide\\_Introduction](https://www.owasp.org/index.php/Testing_Guide_Introduction)

# Zero Day Vulnerability

Window of exposure =  $\infty$

[https://en.wikipedia.org/wiki/Zero-day\\_\(computing\)](https://en.wikipedia.org/wiki/Zero-day_(computing))

Una vulnerabilità scoperta ma non resa pubblica (nemmeno al produttore).

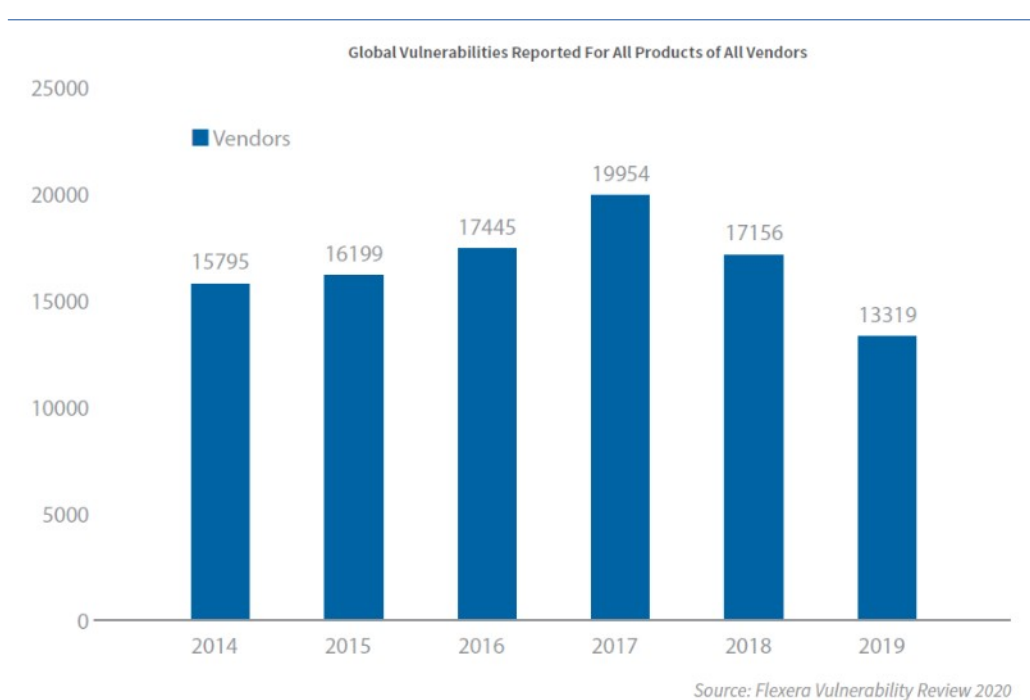
Solitamente rivendute oppure tenute da parte per operazioni redditizie (anche governative).

Window of exposure infinita (o almeno finché qualcuno non se ne accorge).

Business nemmeno più nascosto

<https://zerodium.com/>

## Vulnerabilità



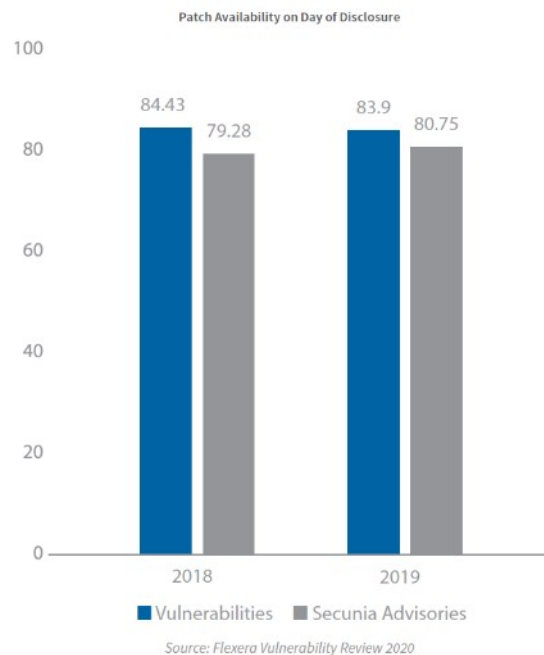
Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

5

Fonte Flexera Vulnerability review 2020  
<https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020>

Tendenza al miglioramento.

## Vulnerabilità



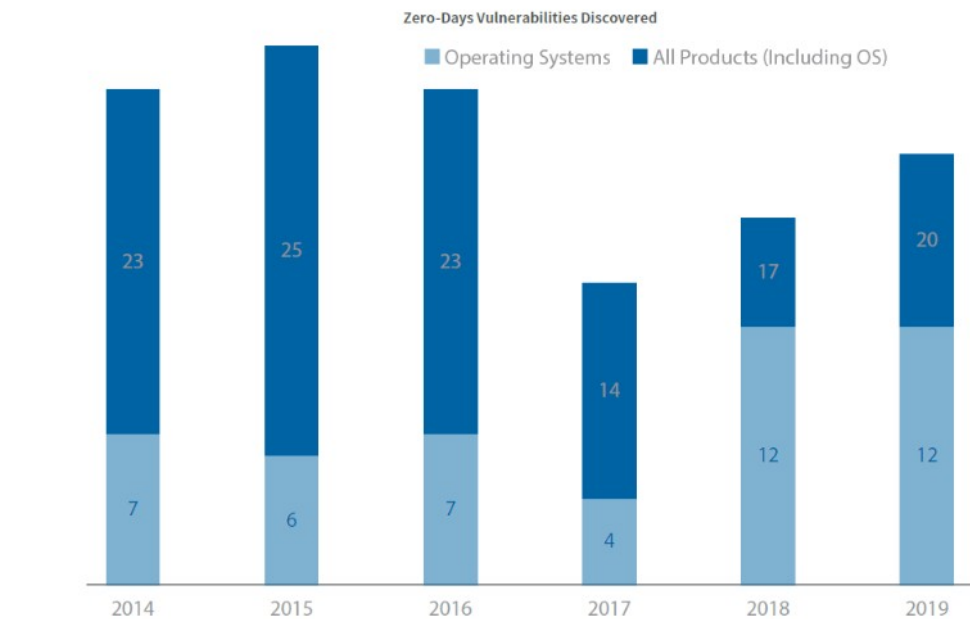
Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

6

Fonte Flexera Vulnerability review 2020  
<https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020>

Nell'84% dei casi patch disponibile il giorno stesso della segnalazione della vulnerabilità. Il rimanente 16% probabilmente non verrà mai patchato (vendor non esiste più, software fuori manutenzione ecc.)

## Vulnerabilità



Source: Flexera Vulnerability Review 2020

Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

7

Fonte Flexera Vulnerability review 2020  
<https://info.flexera.com/SVM-REPORT-Vulnerability-Review-2020>

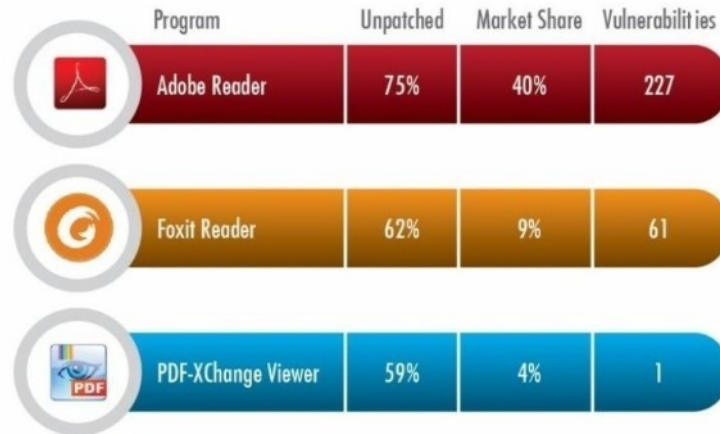
Pochi zero day scoperti: perché chi li ha scoperti è bravo a tenerli segreti? (se li uso in un attacco rischio di farmi scoprire e di perdere lo zero day)

# Vulnerabilità

Figure  
26

## PDF READER MARKET SHARE/UNPATCHED SHARE/NUMBER OF VULNERABILITIES

Vulnerabilities indicate the number of new vulnerabilities in the last 12 months.  
Market share is percentage of Personal Software Inspector users with the product installed on their PC.



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

8

Fonte Flexera Vulnerability review 2017  
<http://www.flexerasoftware.com/enterprise/resources/research/vulnerability-review/>

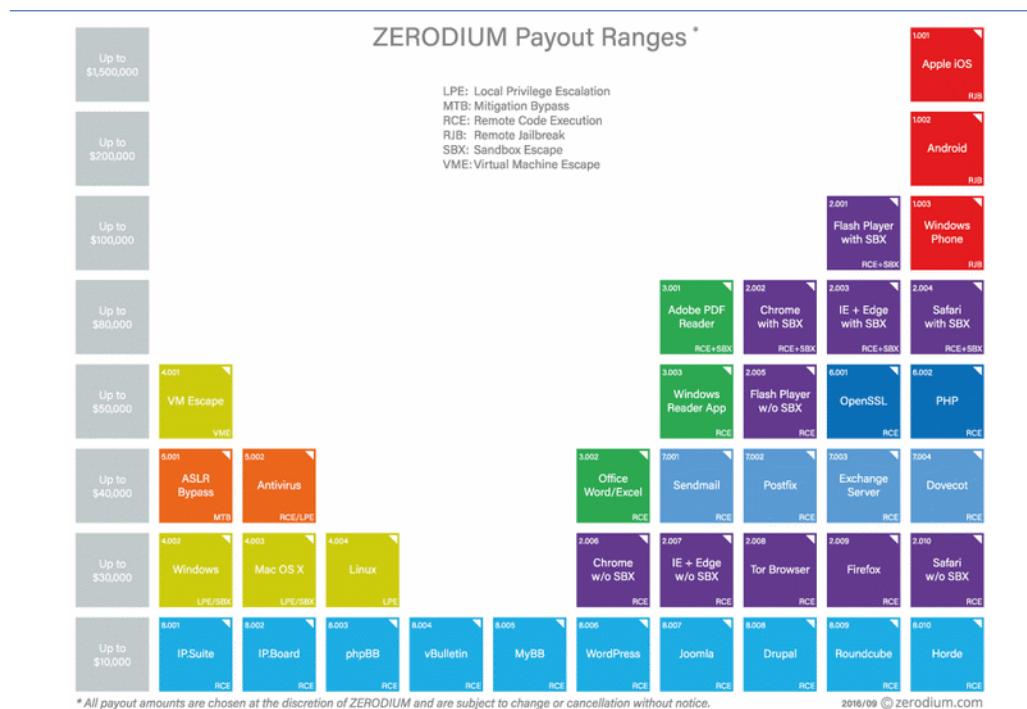
Quindi Acrobat Reader è:

- Diffuso
- Bucato
- Non patchato

Una manna per un attaccante!



# Vulnerabilità



Massimo Carnevali - Licenza Creative Commons 4.0: Attribuzione-Condividi allo stesso modo

Quanto paga Zerodium per una vulnerabilità zero day.  
(vedi anche la parte su “chi sono i cattivi”)

# Patch management

[http://en.wikipedia.org/wiki/Patch\\_\(computing\)](http://en.wikipedia.org/wiki/Patch_(computing))

E' un sottoproblema del configuration management di particolare impatto sulle metodologie per la sicurezza dei sistemi.

To patch or not to patch?

Questa domanda ha una risposta risolvendo il problema seguente:  
il rischio di applicare al sistema la patch è superiore al rischio della vulnerabilità che la patch corregge?

E' un calcolo difficile e comunque deve essere effettuato all'interno di una metodologia chiara e ben pianificata.

Una corretta metodologia di patch management può essere espressa in varie fasi

1. Baseline definition
2. Test Environments
3. Backout Plans
4. Patch collection and evaluation
5. Consolidation
6. Deployment
7. Reporting