

Programmazione Sicura



Catalogazione
delle vulnerabilità

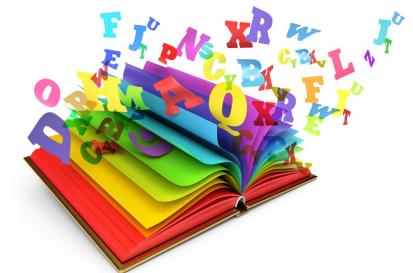


Barbara Masucci
UNIVERSITÀ DEGLI STUDI DI SALERNO
DIPARTIMENTO DI INFORMATICA
DIPARTIMENTO DI ECCELLENZA



Punto della situazione

- La volta scorsa abbiamo fornito una **panoramica storica** su diversi tipi di incidenti e introdotto la **terminologia necessaria** ai nostri scopi



- **Scopo della lezione di oggi:**
 - Analizzare il ciclo di vita delle **vulnerabilità del software**
 - Descrivere un sistema di catalogazione delle vulnerabilità: **CVE**
 - Descrivere un sistema di catalogazione delle vulnerabilità, basato su metriche: **CVSS**



Vulnerabilità del software

- Per **vulnerabilità** si intende una debolezza presente, comprensibile e sfruttabile da un attaccante
- Vediamo il **ciclo di vita** di una vulnerabilità:
 - Rilascio di un software da un venditore
 - Scoperta della vulnerabilità da parte di un attaccante e rilascio di un exploit
 - Scoperta della vulnerabilità da parte del venditore
 - Divulgazione della vulnerabilità al pubblico
 - Rilevazione dell'exploit da parte degli anti-virus
 - Rilascio di una patch da parte del venditore
 - Mitigazione dell'exploit su tutti i sistemi



Ciclo di vita di una vulnerabilità

Un fornitore rilascia una nuova versione di un software con una vulnerabilità

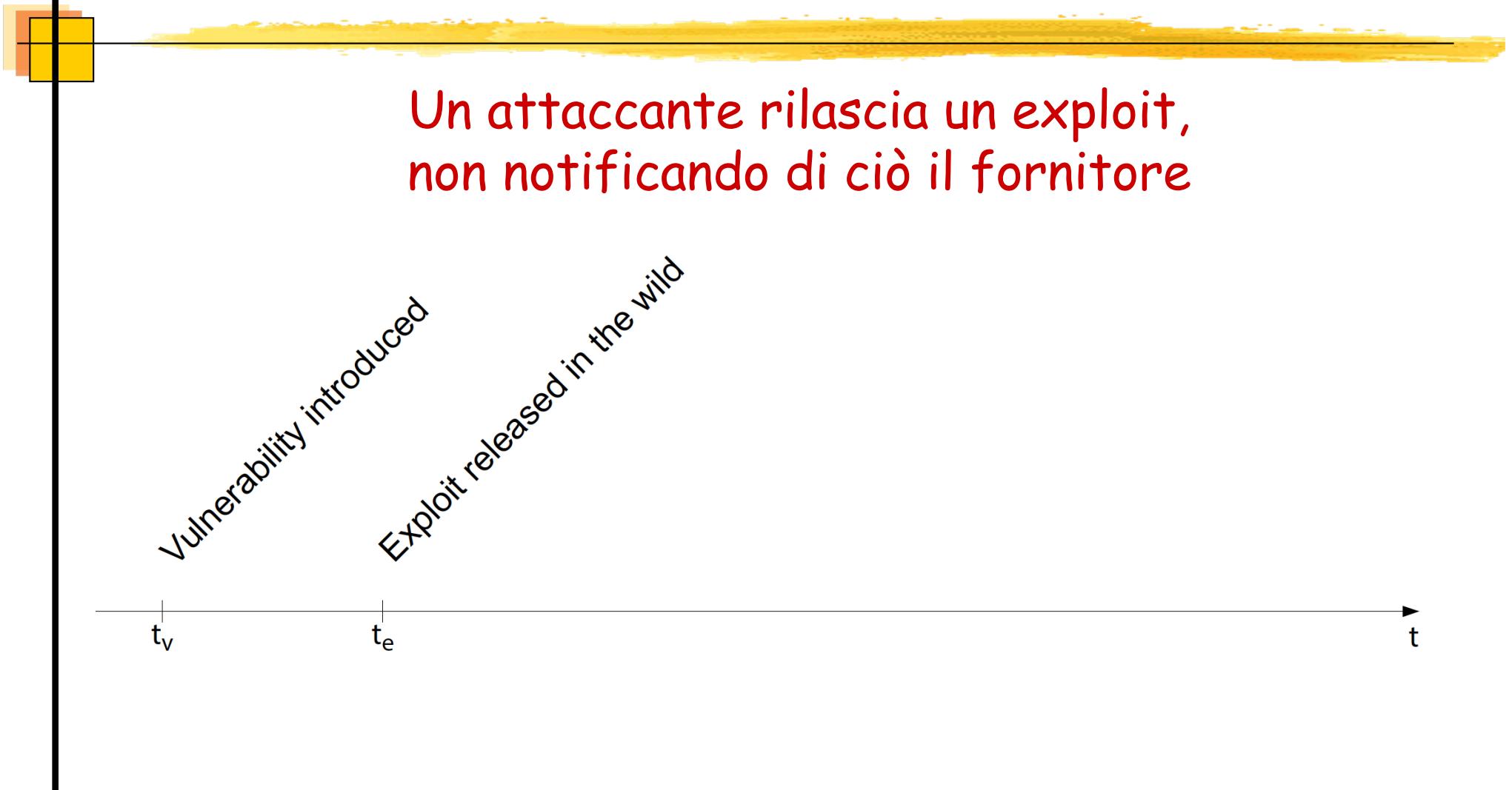
Vulnerability introduced

t_v

t

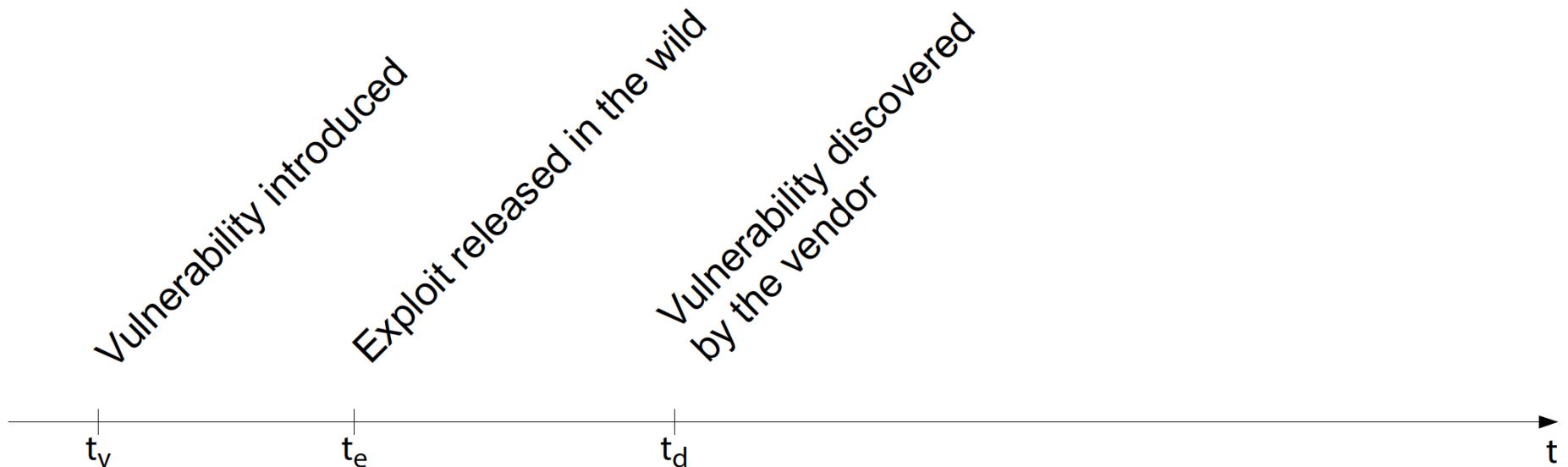


Ciclo di vita di una vulnerabilità



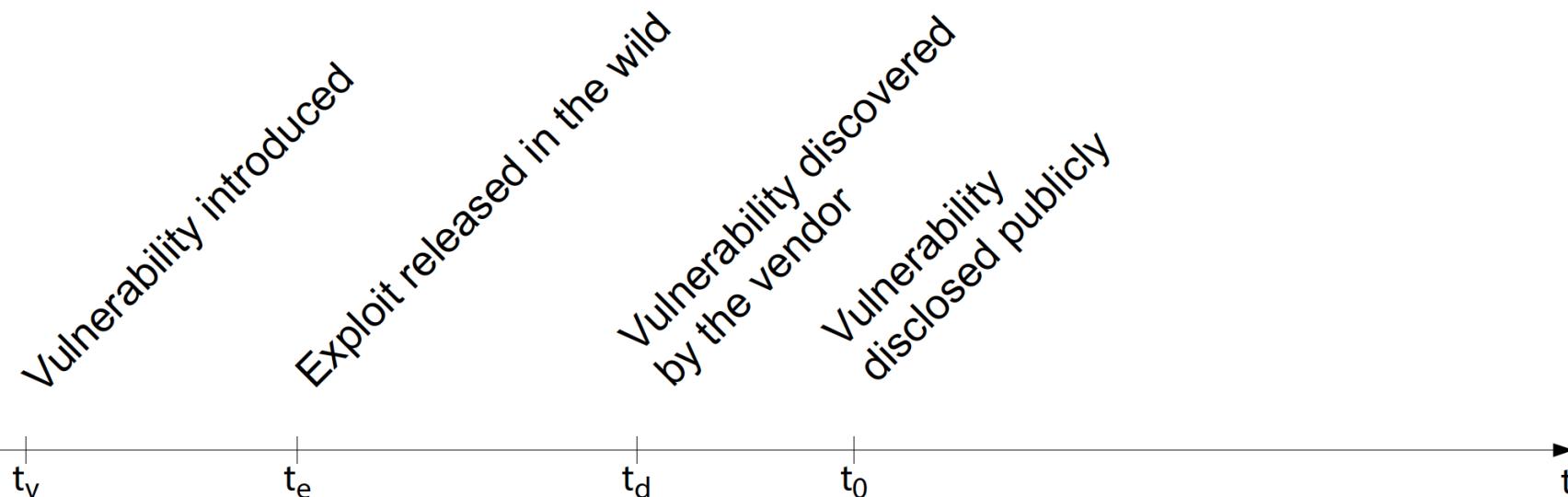
Ciclo di vita di una vulnerabilità

Il fornitore si accorge dell'exploit,
in proprio o tramite segnalazione



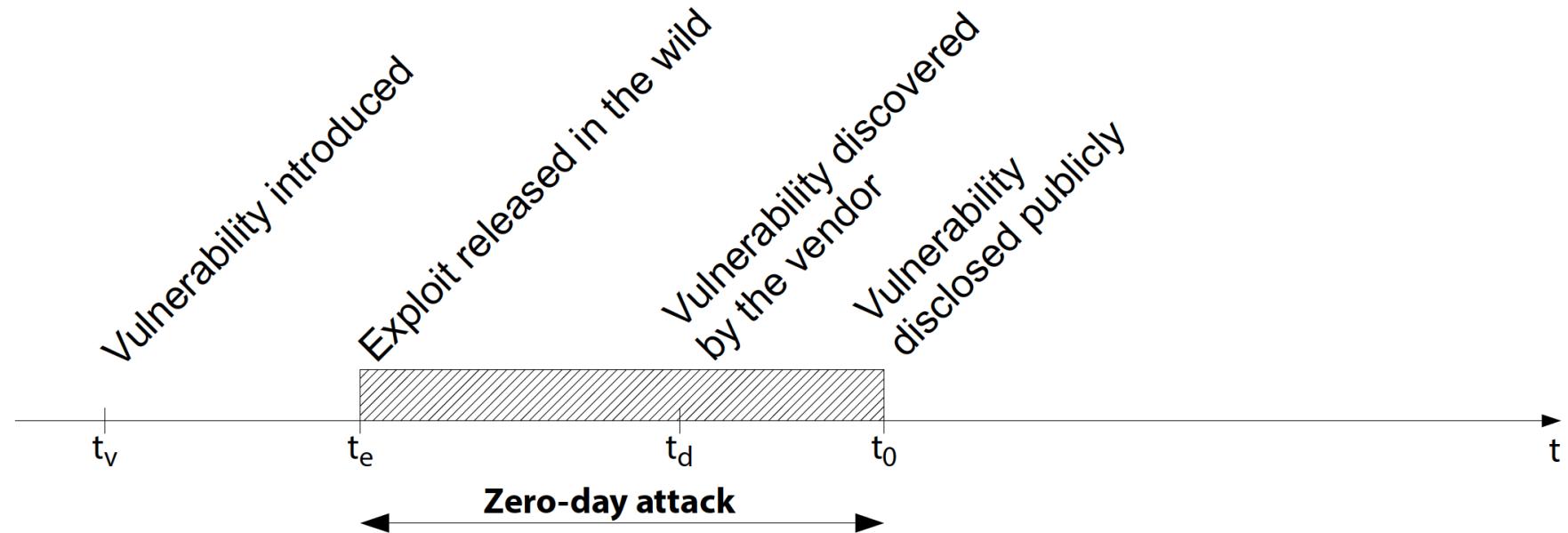
Ciclo di vita di una vulnerabilità

La vulnerabilità è divulgata pubblicamente



Ciclo di vita di una vulnerabilità

Nell'intervallo $[t_e, t_0]$ la vulnerabilità è stata sfruttata nell'oscurità

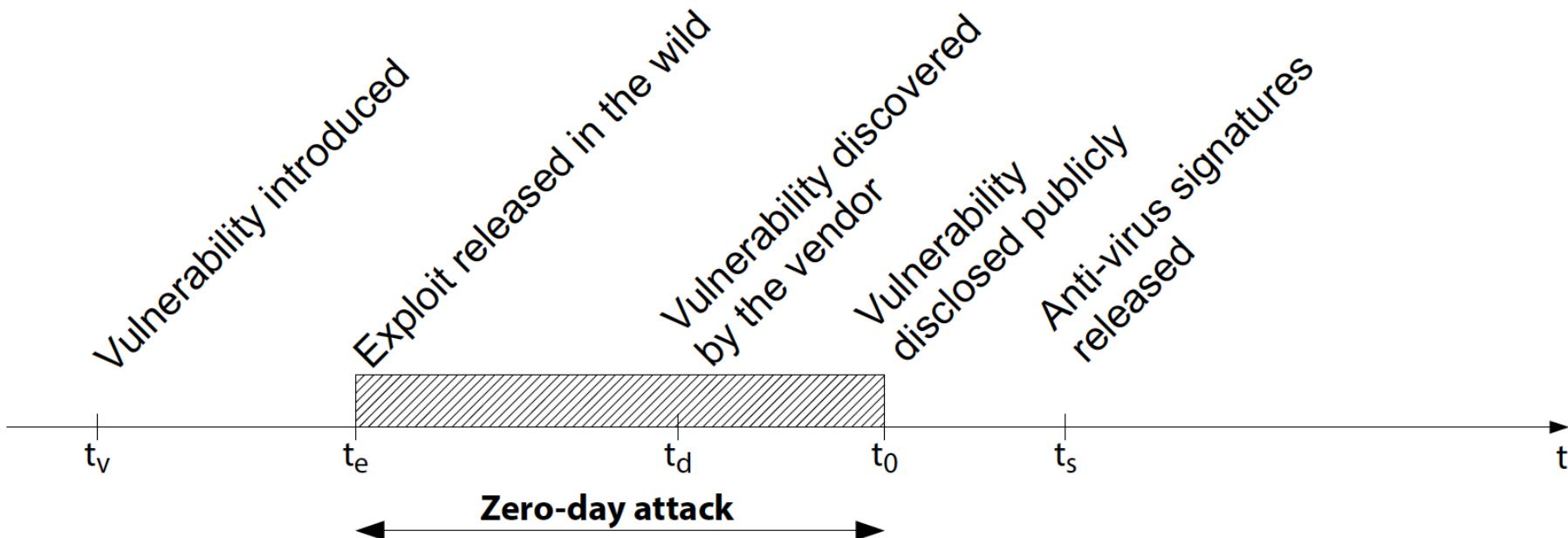


L'attacco effettuato nel periodo $[t_e, t_0]$ viene detto **zero-day attack**

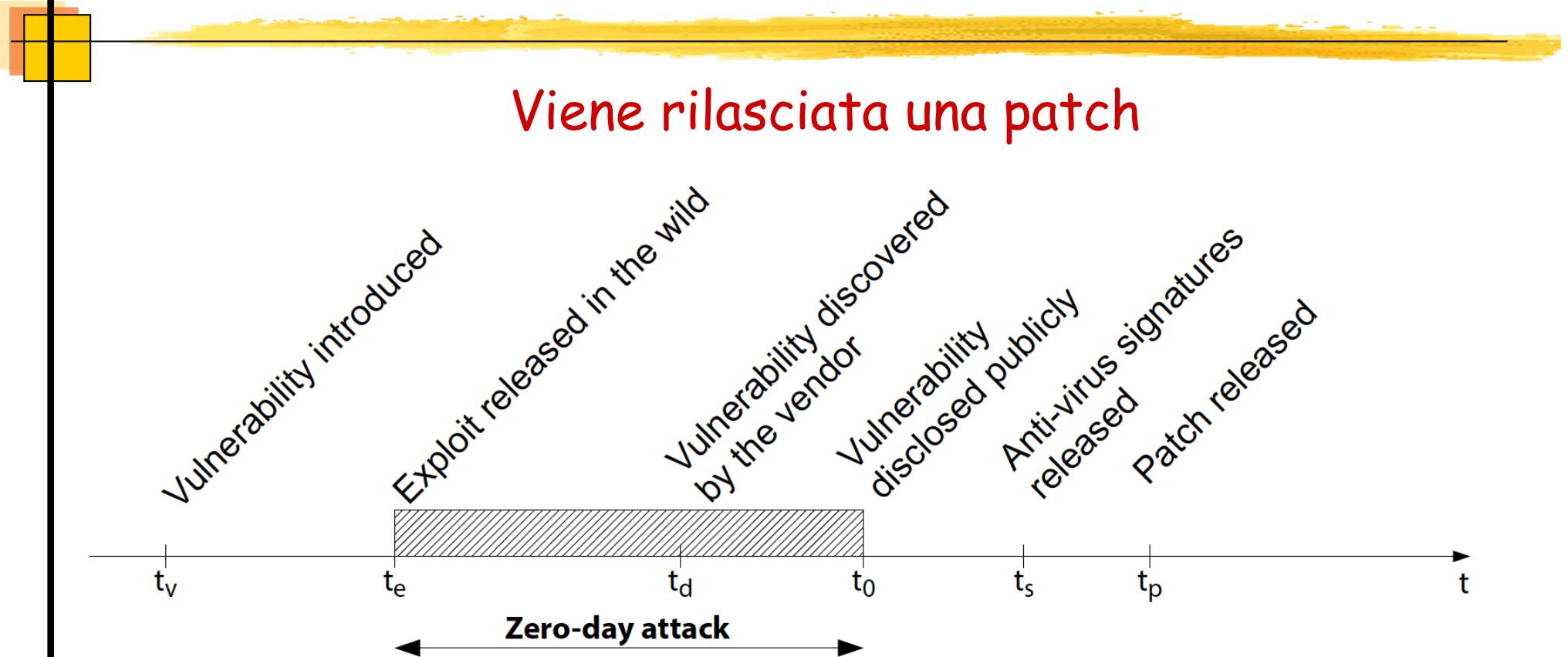


Ciclo di vita di una vulnerabilità

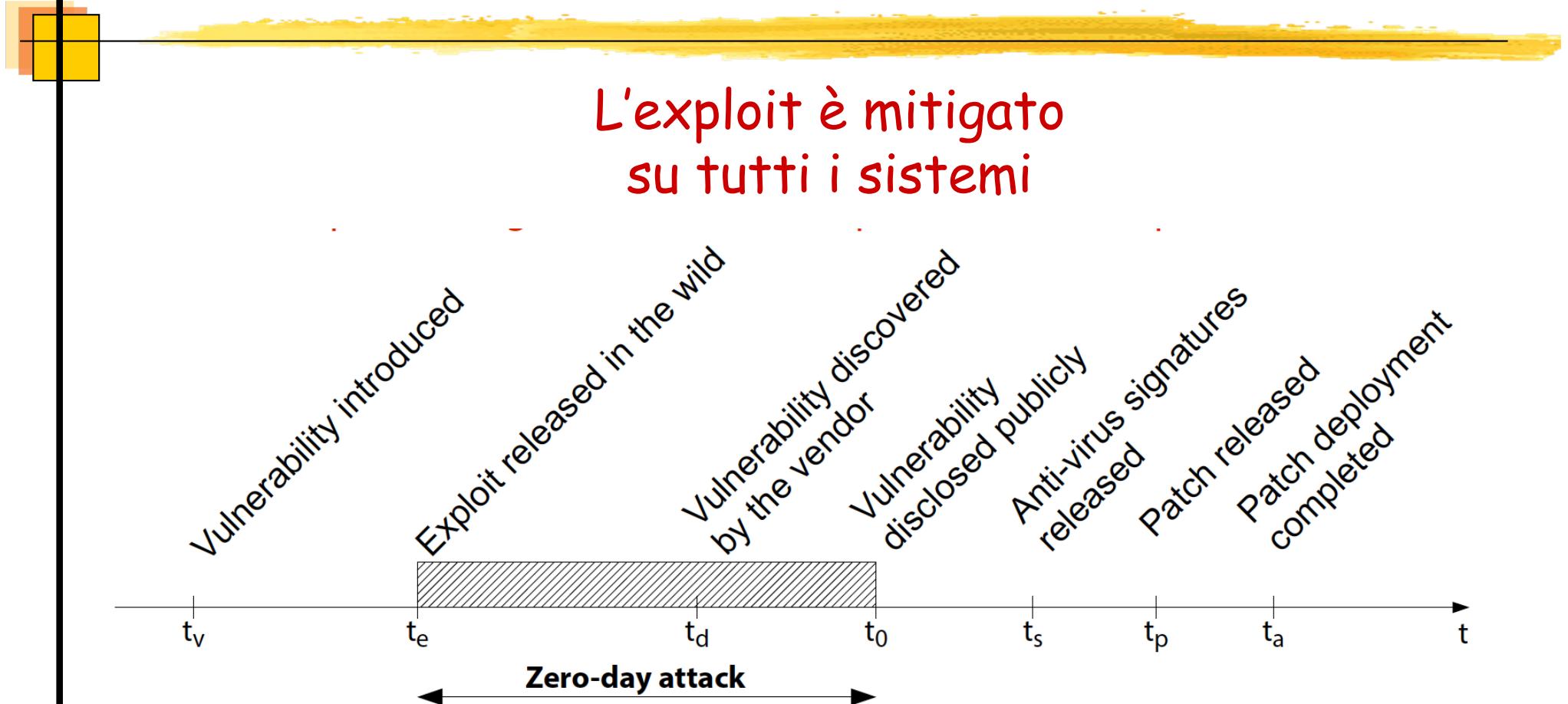
Gli anti-virus sono in grado
di rivelare l'exploit



Ciclo di vita di una vulnerabilità

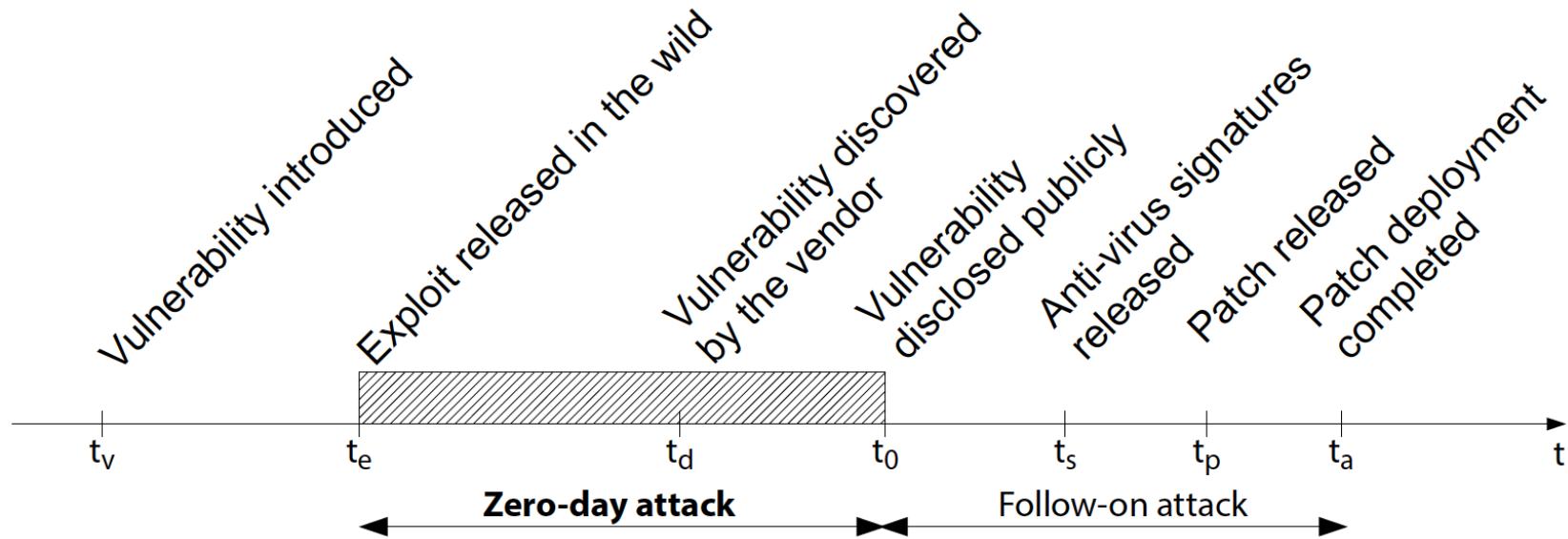


Ciclo di vita di una vulnerabilità



Ciclo di vita di una vulnerabilità

Nell'intervallo $[t_0, t_a]$ la vulnerabilità
è stata sfruttata pubblicamente

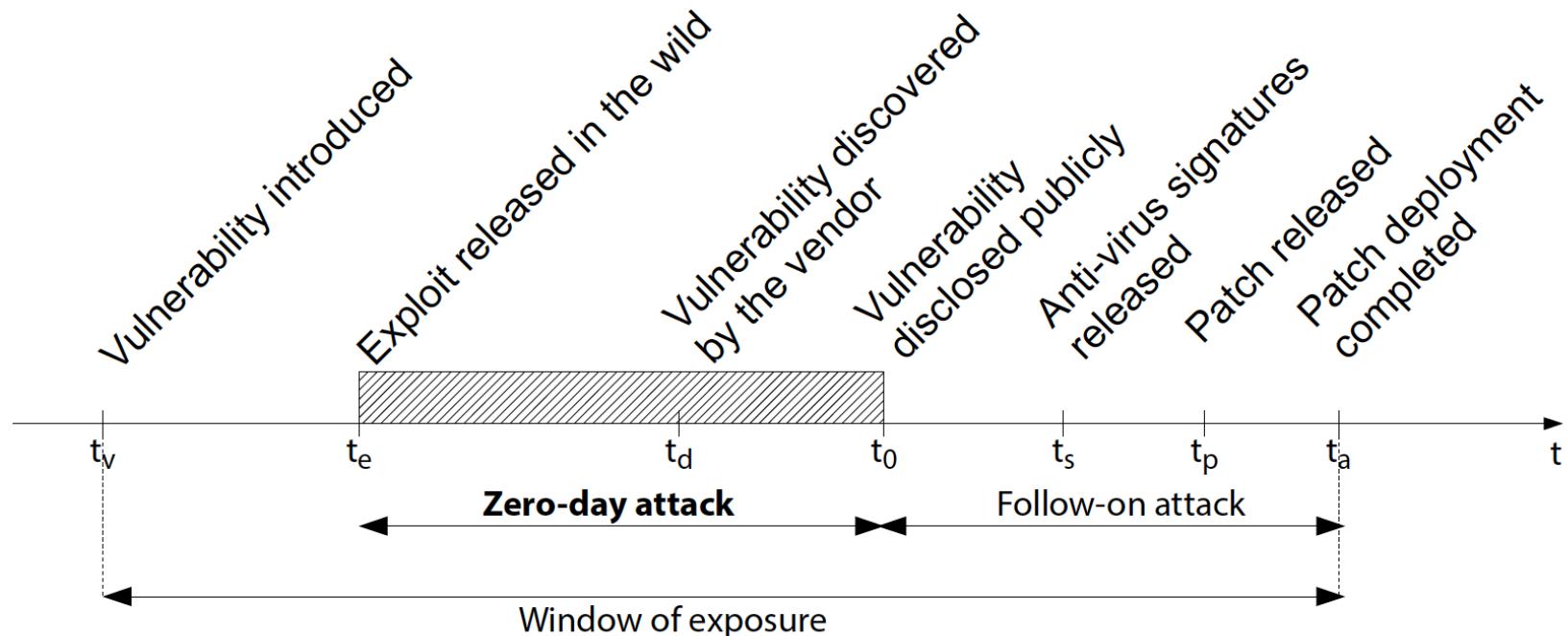


L'attacco effettuato nel periodo $[t_0, t_a]$
avviene in presenza della conoscenza
pubblica della vulnerabilità



Ciclo di vita di una vulnerabilità

L'intervallo $[t_v, t_a]$ costituisce la finestra di esposizione della vulnerabilità



Più vicini si è allo **zero-day**, più è probabile che un attacco al software abbia successo



Zerodium

- Azienda di sicurezza informatica fondata nel 2015
- Offre ricompense fino a **\$2.500.000** a chi fornisce **zero-day exploit**



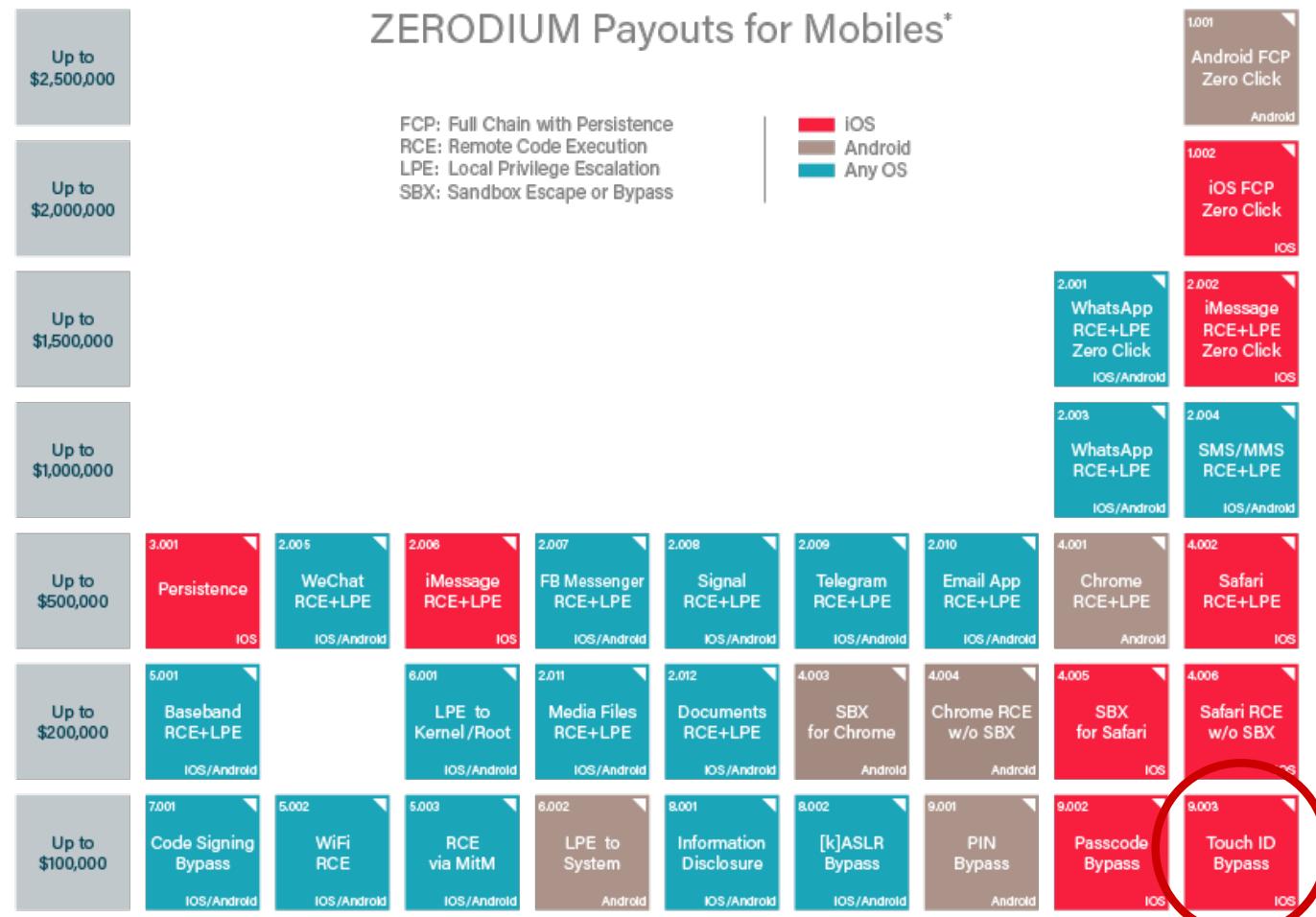
www.zerodium.com



Zero-day exploit su mobile

Settembre 2019

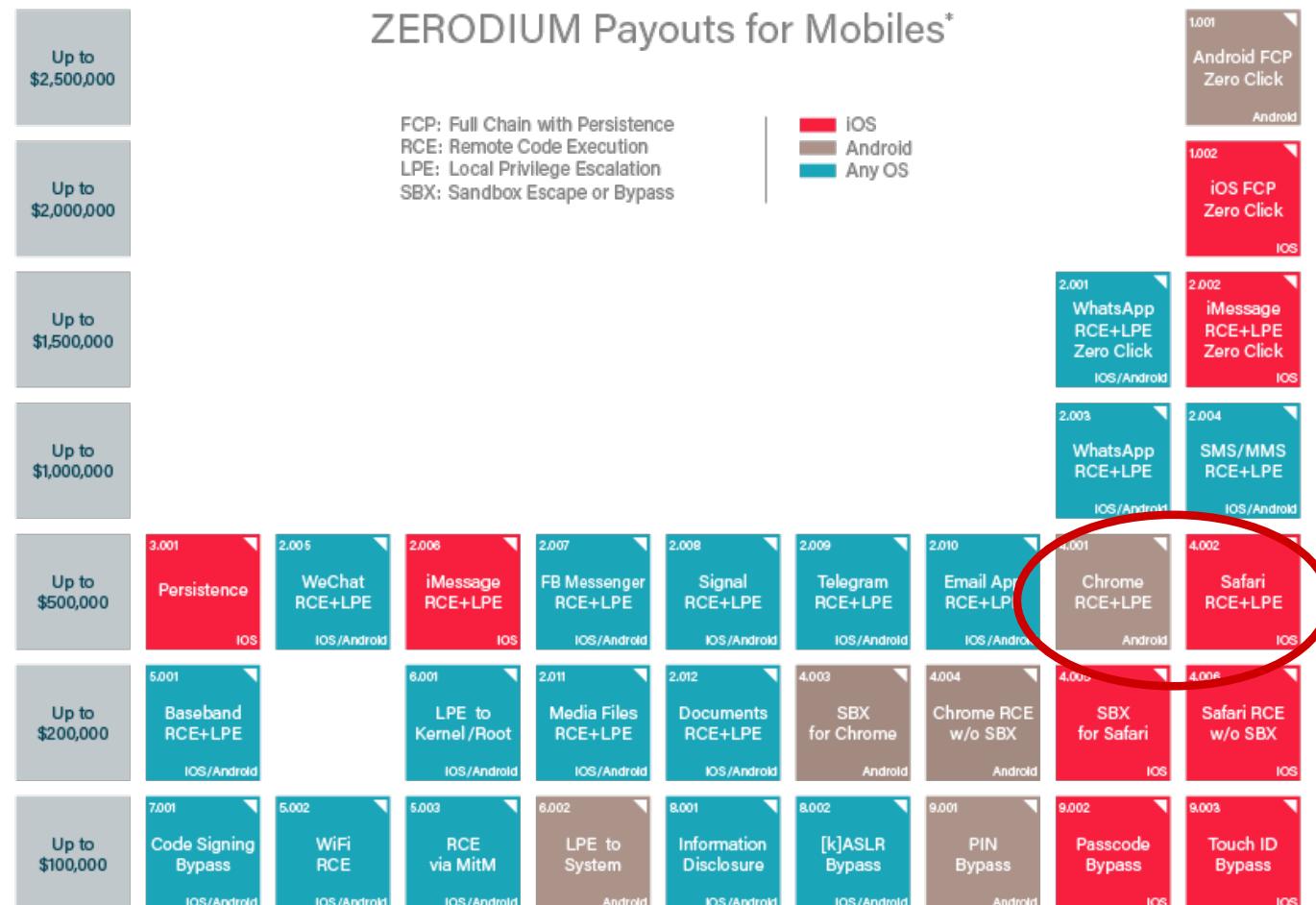
Un attacco di **bypass** del Touch-ID su iOS è
“economico” (può valere fino a \$100.000)



Zero-day exploit su mobile

Settembre 2019

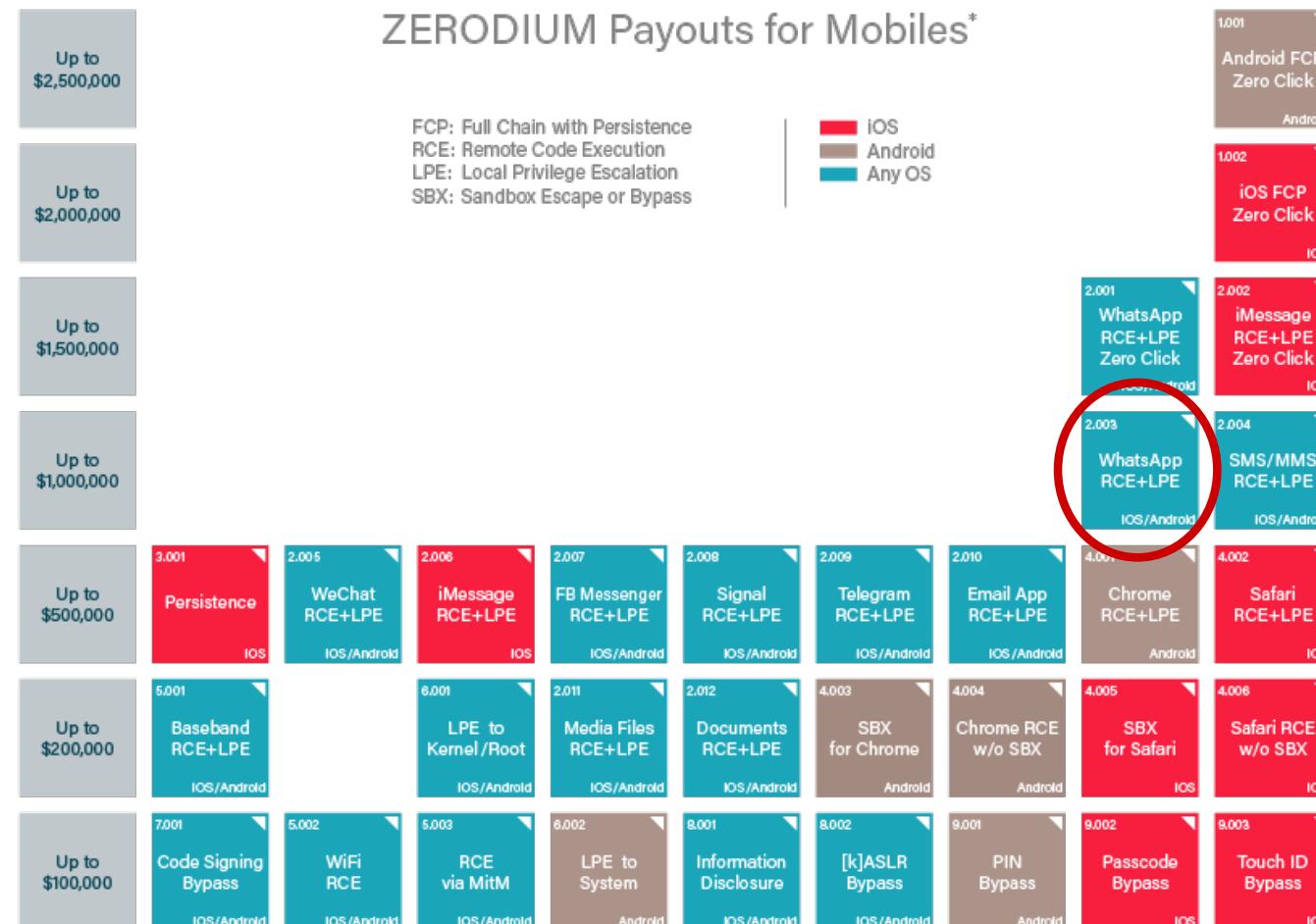
Un attacco contro **Chrome** o **Safari** può valere
5 volte tanto (fino a **\$500.000**)



Zero-day exploit su mobile

Settembre 2019

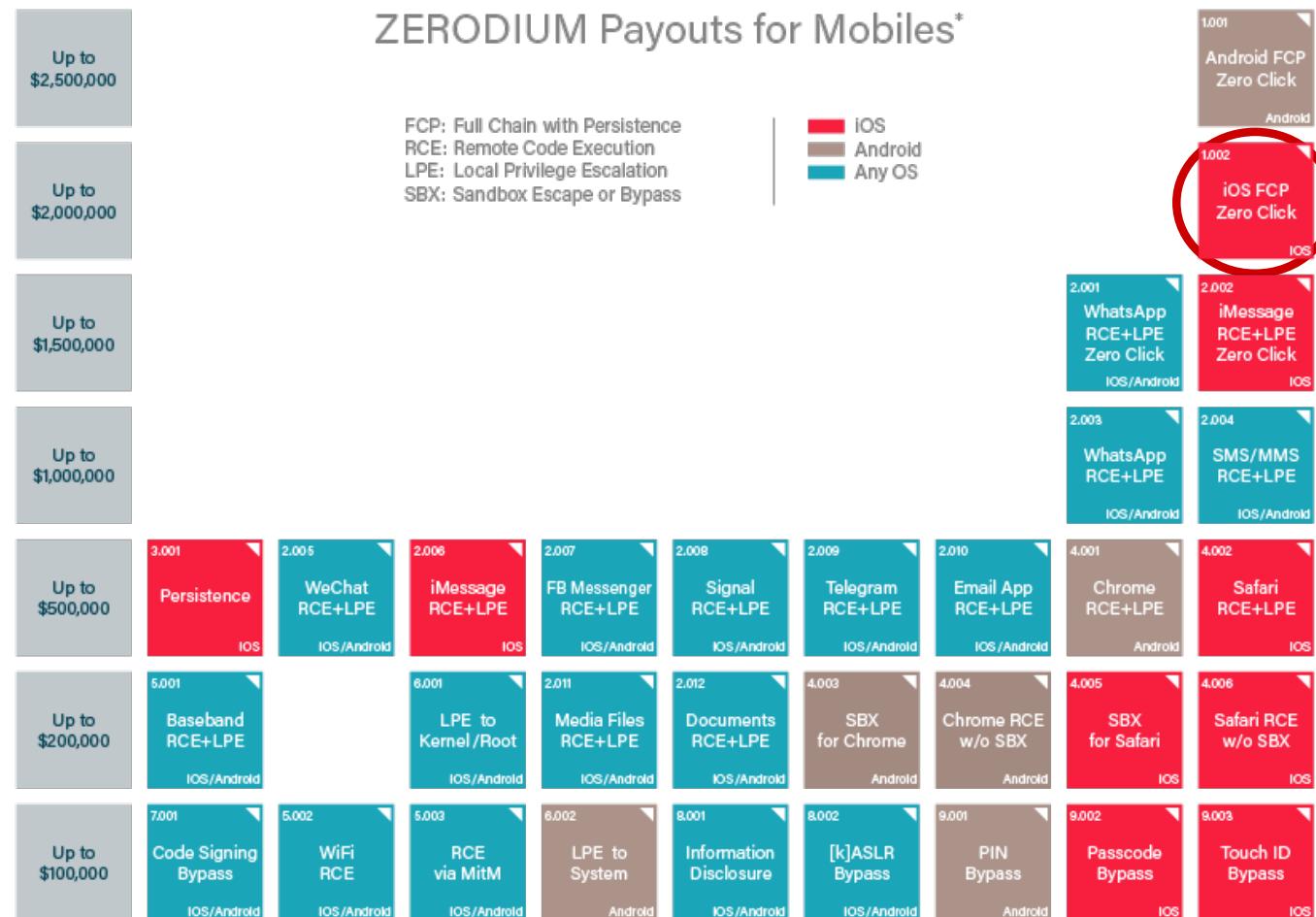
Un attacco contro WhatsApp può valere
10 volte tanto (fino a \$1.000.000)



Zero-day exploit su mobile

Settembre 2019

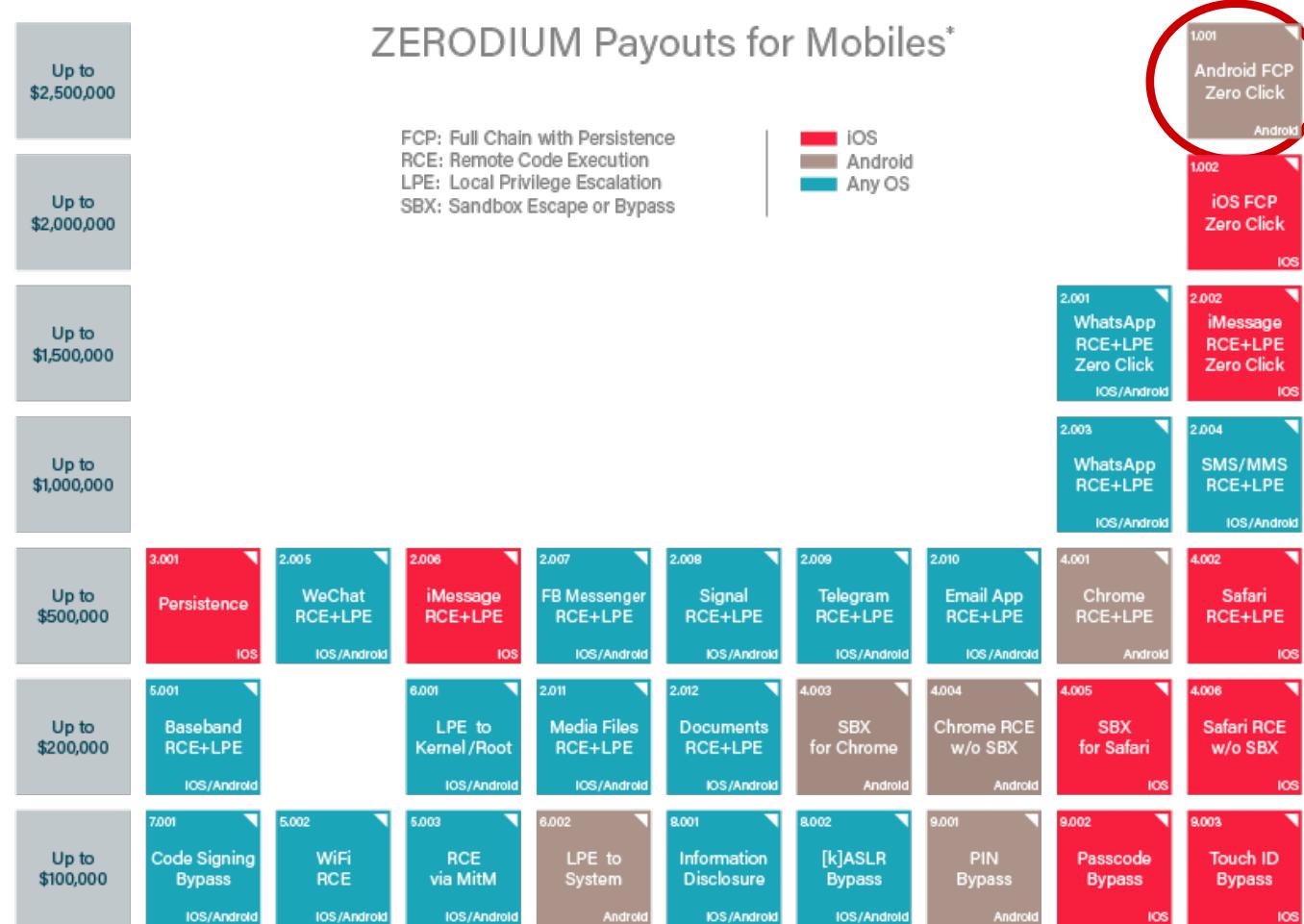
Un attacco **Zero-Click** contro **iOS** può valere
20 volte tanto (fino a **\$2.000.000**)



Zero-day exploit su mobile

Settembre 2019

Un attacco **Zero-Click** contro **Android** può valere
25 volte tanto (fino a **\$2.500.000**)



Zero-day exploit su mobile

Maggio 2020

- Nel 2015 Zerodium è arrivata ad offrire un milione di dollari per attacchi zero-day contro iOS 9
- A Maggio 2020 Zerodium ha annunciato con un tweet di non essere più interessata ad exploit contro iOS

 @Zerodium

We will NOT be acquiring any new Apple iOS LPE, Safari RCE, or sandbox escapes for the next 2 to 3 months due to a high number of submissions related to these vectors.

Prices for iOS one-click chains (e.g. via Safari) without persistence will likely drop in the near future.

2:11 PM · 13 mag 2020

(i)

- Le prime avvisaglie di questo cambio di rotta si erano già avute con l'aggiornamento dei "listini" che mostravano maggior interesse per Android



Zero-day exploit su mobile

Ottobre 2021

- Nel 2021 Zerodium ha mostrato interesse verso exploit per i servizi di **VPN di Windows**

 Zerodium 
@Zerodium

We're looking for **#0day** exploits affecting VPN software for Windows:

- ExpressVPN
- NordVPN
- Surfshark

Exploit types: information disclosure, IP address leak, or remote code execution. Local privilege escalation is out of scope.



- In particolare, interessano exploit che portino a
 - esposizione di informazioni confidenziali
 - violazione dell'anonimato
 - esecuzione di codice arbitrario



Zero-day exploit su mobile

Gennaio 2022

- Nel 2022 Zerodium ha aumentato l'offerta per exploit contro popolari client di posta elettronica, come Mozilla Thunderbird e Microsoft Outlook



We're currently paying up to \$200,000 per exploit for Mozilla Thunderbird RCEs.

We're also (temporarily) increasing our bounty for MS Outlook RCEs to \$400,000 (from \$250,000).

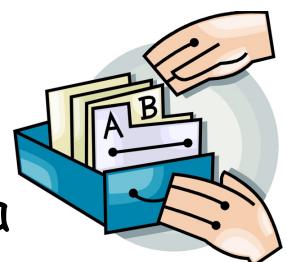
More details at: zerodium.com/temporary.html

8:06 PM · Jan 27, 2022 · Twitter Web App



Catalogare le vulnerabilità

- E' importante tenere traccia delle vulnerabilità note
- Ciò può essere fatto mediante
 - **Enumerazione**
Costruzione di una tupla univoca per ciascuna vulnerabilità:
(id, tipo vulnerabilità, vettore di attacco, minaccia, exploit)
 - **Catalogazione**
Inserimento della tupla in un archivio
- Sono stati proposti diversi archivi indipendenti
 - Problemi: duplicazione, eterogeneità
 - Nel 1998 la stessa vulnerabilità è stata catalogata 12 volte da team differenti



Catalogare le vulnerabilità

PHF phonebook CGI vulnerability: 12 catalogazioni

Table 1 - Vulnerability Tower of Babel, 1998

Organization	Name referring to vulnerability
AXENT (now Symantec)	phf CGI allows remote command execution
BindView	#107-cgi-phf
Bugtraq	PHF Attacks-fun and games for the whole family
CERIAS	http_escshellcmd
CERT	CA-96.06.cgi_example_code
Cisco Systems	HTTP-cgi-phf
CyberSafe	Network: HTTP 'phf' attack
DARPA	0x00000025 = HTTP PHF attack
IBM ERS	ERS-SVA-E01-1996:002.1
ISS	http-cgi-phf
Symantec	#180 HTTP server CGI example code compromises http server
SecurityFocus	#629-phf Remote Command Execution Vulnerability



Common Vulnerability Exposure

- Nel 1999 il **MITRE**, un ente no-profit, ha introdotto un catalogo uniforme delle vulnerabilità
 - **Common Vulnerability Exposures (CVE)** disponibile al link <https://cve.org>
- Le vulnerabilità presenti nel CVE
 - Violano almeno una proprietà nella triade CIA (Confidentiality, Integrity, Availability)
 - Sono identificate da una stringa univoca **CVE-ANNO-NUMERO**
 - Sono descritte da una scheda esplicativa contenente
 - Descrizione
 - URL a una pagina dettagliata (References)
 - Data di creazione



Esempio: CVE-2014-0160

Scheda della vulnerabilità CVE-2014-0160

CVE-ID	Learn more at National Vulnerability Database (NVD)
CVE-2014-0160	<ul style="list-style-type: none">CVSS Severity RatingFix InformationVulnerable Software VersionsSCAP MappingsCPE Information
Description	The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.

Il CVE id

Una descrizione dettagliata
della vulnerabilità.



Esempio: CVE-2014-0160

Scheda della vulnerabilità CVE-2014-0160 (References)

Un elenco di URL descrivente la vulnerabilità in maggiore dettaglio.
URL diversi sono redatti da team di sicurezza diversi:
associati al software;
associati alla distribuzione;
Indipendenti.

CVE-ID	Learn more at National Vulnerability Database (NVD)
CVE-2014-0160	• CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
The (1) TLS and (2) DTLS implementations in OpenSSL 1.0.1 before 1.0.1g do not properly handle Heartbeat Extension packets, which allows remote attackers to obtain sensitive information from process memory via crafted packets that trigger a buffer over-read, as demonstrated by reading private keys, related to d1_both.c and t1_lib.c, aka the Heartbleed bug.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
<ul style="list-style-type: none">• BUGTRAQ:20141205 NEW: VMSA-2014-0012 - VMware vSphere product updates address security vulnerabilities• URL:http://www.securityfocus.com/archive/1/archive/1/534161/100/0/threaded• EXPLOIT-DB:32745• URL:http://www.exploit-db.com/exploits/32745• EXPLOIT-DB:32764• URL:http://www.exploit-db.com/exploits/32764• FULLDISC:20140408 Re: heartbleed OpenSSL bug CVE-2014-0160• URL:http://seclists.org/fulldisclosure/2014/Apr/91• FULLDISC:20140408 heartbleed OpenSSL bug CVE-2014-0160• URL:http://seclists.org/fulldisclosure/2014/Apr/90• FULLDISC:20140409 Re: heartbleed OpenSSL bug CVE-2014-0160• URL:http://seclists.org/fulldisclosure/2014/Apr/92	

La data di creazione del CVE id, in formato YYYYMMDD.

Date Entry Created
20131203
Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.



Esempio: CVE-2014-0160

➤ Si tratta di una vulnerabilità della **libreria crittografica Open SSL**, resa nota al pubblico nell'Aprile 2014



- OpenSSL, fin dal 1998, è largamente utilizzata nelle applicazioni Web per la protezione delle informazioni scambiate tra client e server
- Tale vulnerabilità, detta "**Heartbleed**",
consentiva di **violare la confidenzialità delle informazioni** protette mediante il protocollo SSL/TLS
 - Oltre il 60% dei server Web era vulnerabile all'attacco
 - Successivamente fu rilasciata una nuova versione di OpenSSL che eliminava il difetto



Heartbleed

The 'Heartbleed' security flaw that affects most of the Internet

By Heather Kelly, CNN

Updated 2111 GMT (0511 HKT) April 9, 2014



News Sport Weather Shop Earth Travel More

NEWS

Home | Video | World | UK | Business | Tech | Science | Stories | Entertainment & Arts | Help

Technology

Heartbleed bug: What you need to know

NETWORK ▾ L'Espresso | R2 LE INCHIESTE



Tecnologia

f t m Share

Home

News

Speciali

Mobile

Social Network

Sicurezza

Consiglia 1,6 mila Condivi

Internet, falla in OpenSSL: 'Heartbleed' mette a rischio password e carte di credito in due terzi dei siti web



Come funziona Heartbleed?

- Heartbleed è causata da una **impropria validazione degli input** all'interno dell'implementazione della estensione heartbeat di TLS
 - Usando tale estensione, ciascuna delle due parti comunicanti conferma all'altra la propria presenza inviando un pacchetto (**heartbeat payload**) contenente alcuni dati testuali
 - L'attacco consiste nell'inviare informazioni false relative alla lunghezza del payload
 - Dichiarando che la **lunghezza del payload è la massima possibile** (64KB), il server che riceve il pacchetto risponde copiando la quantità di memoria richiesta
 - **Tale memoria può contenere qualsiasi cosa** (chiavi di cifratura, password, etc.)

Esempio di Mancata Validazione degli Input

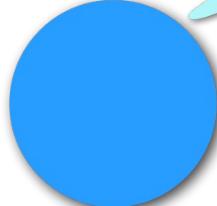


Come funziona Heartbleed?



Heartbeat – Normal usage

Client



Server, send me
this 4 letter word
if you are there:
"bird"

bird

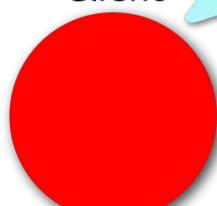
Server

has connected.
User Bob has
connected. User
Alice wants 4
letters: **bird**. Serve
master key is
31431498531054.
User Carol wants to
change password
"password 123" ...



Heartbeat – Malicious usage

Client



Server, send me
this 500 letter
word if you are
there: "bird"

bird. Server
master key is
31431498531054.
User Carol wants
to change
password to
"password 123" ...

Server

has connected.
User Bob has
connected. User
Mallory wants 500
letters: **bird**. Serve
master key is
31431498531054.
User Carol wants to
change password
"password 123" ...



Esempio: CVE-2014-6271

Scheda della vulnerabilità CVE-2014-6271

Il CVE id →

Una descrizione dettagliata della vulnerabilità. →

CVE-ID
CVE-2014-6271 Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description
GNU Bash through 4.3 processes trailing strings after function definitions in the values of environment variables, which allows remote attackers to execute arbitrary code via a crafted environment, as demonstrated by vectors involving the ForceCommand feature in OpenSSH sshd, the mod_cgi and mod_cgid modules in the Apache HTTP Server, scripts executed by unspecified DHCP clients, and other situations in which setting the environment occurs across a privilege boundary from Bash execution, aka "ShellShock." NOTE: the original fix for this issue was incorrect; CVE-2014-7169 has been assigned to cover the vulnerability that is still present after the incorrect fix.



Esempio: CVE-2014-6271

Scheda della vulnerabilità CVE-2014-6271 (References)

Un elenco di URL descrivente la vulnerabilità in maggiore dettaglio.
URL diversi sono redatti da team di sicurezza diversi:
associati al software;
associati alla distribuzione;
Indipendenti.

References

Note: [References](#) are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.

- BUGTRAQ:20141001 NEW VMSA-2014-0010 - VMware product updates address critical Bash security vulnerabilities
- URL:<http://www.securityfocus.com/archive/1/archive/1/533593/100/0/threaded>
- EXPLOIT-DB:39918
- URL:<https://www.exploit-db.com/exploits/39918/>
- FULLDISC:20141001 FW: NEW VMSA-2014-0010 - VMware product updates address critical Bash security vulnerabilities
- URL:<http://seclists.org/fulldisclosure/2014/Oct/0>
- MISC:<http://lcamtuf.blogspot.com/2014/09/quick-notes-about-bash-bug-its-impact.html>
- MISC:<http://packetstormsecurity.com/files/128517/VMware-Security-Advisory-2014-0010.html>
- MISC:<http://packetstormsecurity.com/files/128567/CA-Technologies-GNU-Bash-Shellshock.html>
- MISC:http://packetstormsecurity.com/files/128573/Apache-mod_cgi-Remote-Command-Execution.html
- MISC:<http://packetstormsecurity.com/files/137376/IPFire-Bash-Environment-Variable-Injection-Shellshock.html>

...

Date Entry Created

20140909

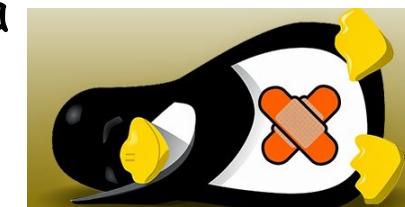
Disclaimer: The entry creation date may reflect when the CVE-ID was allocated or reserved, and does not necessarily indicate when this vulnerability was discovered, shared with the affected vendor, publicly disclosed, or updated in CVE.

La data di creazione del CVE id,
in formato YYYYMMDD.



Esempio: CVE-2014-6271

- Si tratta di una vulnerabilità della **shell BASH**, resa nota al pubblico nel Settembre 2014
 - BASH, proposta nel 1989 in sostituzione della Bourne shell, è la shell di default per molte distribuzioni Linux e MacOs
- Tale vulnerabilità, detta "**Shellshock**", consentiva l'esecuzione di codice arbitrario anche da remoto!
 - Nel giro di pochi giorni furono portati a termine **milioni di attacchi**, principalmente di tipo DDoS
 - Successivamente fu rilasciata una nuova versione della shell BASH che eliminava il difetto



Shellshock

BBC NEWS: Shellshock: 'Deadly serious' new vulnerability found

By Dave Lee
Technology reporter, BBC News
© 25 September 2014 | Technology

Rit Tecnologia: "Shellshock", il virus che minaccia i sistemi Linux ed Apple

Schneier on Security: Nasty Vulnerability found in Bash
It's a big and nasty one.

CNN tech: 'Bash' bug could let hackers attack through a light bulb

by Jose Pagliery @Jose_Pagliery
September 25, 2014: 12:54 PM ET

Bash gets shellshocked

By Jake Edge
October 1, 2014

It's been a crazy week for the [Bash shell](#), its maintainer, and many Linux distributions that use the shell. A remote code-execution vulnerability that was [reported](#) on September 24 has now morphed into multiple related vulnerabilities, which have now mostly been fixed and updates released by distributions. The vulnerabilities have been dubbed "Shellshock" and the technical (and mainstream) press has had a field day reporting on the incident. It all revolves around a somewhat dubious Bash feature, but the widespread use of Bash in places where it may not really make sense contributed to the severity of the bug.



Come funziona Shellshock?

- BASH consente di **esportare variabili e funzioni di ambiente**, rendendole disponibili alle shell figlie

```
$ export foo='() { echo "In foo"; }'  
$ bash -c 'foo'  
In foo
```

Output della funzione

Invocazione di una shell figlia

Esportazione di una funzione



Come funziona Shellshock?

- Supponiamo di concatenare un altro comando al termine della definizione della funzione `foo`

```
$ export foo='() { echo "In foo"; };  
echo vulnerable'
```

- Cosa accade se viene invocata una shell figlia?

```
$ bash -c 'foo'
```

- Risposta: viene visualizzato

vulnerable

In foo



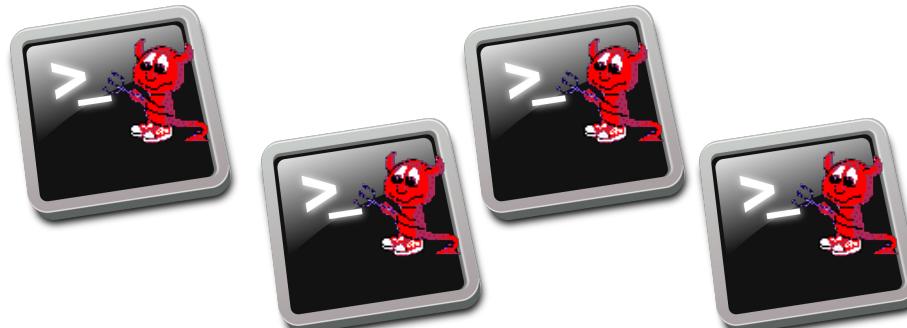
Come funziona Shellshock?

➤ Che conseguenze ha questo fatto?

- Se l'attaccante ha accesso al file di inizializzazione `.bashrc` può inserire la seguente definizione di funzione di ambiente

```
export foo='() { echo "In foo"; }; evil_command'
```

- Ogni volta che l'utente vittima apre una shell BASH viene eseguito il comando **evil_command!**



Esempio di Elevation of Privilege

L'attaccante può eseguire comandi senza esserne autorizzato



Come funziona Shellshock?

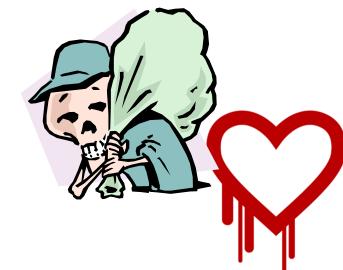
- Ma il problema è ben più serio... perché **l'attacco è eseguibile anche da remoto!**
 - Ogni server remoto che accetta codice BASH e lo valuta senza controllarlo è potenzialmente attaccabile
 - Ad esempio, quando il Web server Apache esegue uno script scritto in BASH, salva gli header della richiesta in variabili di ambiente e le valuta
 - E' sufficiente costruire una linea BASH maligna e passarla come header di una richiesta (maliziosa) per sfruttare la vulnerabilità da remoto...



Shellshock vs Heartbleed

➤ Shellshock è una vulnerabilità molto più seria di Heartbleed

➤ Mentre Heartbleed consente agli attaccanti di rubare dati confidenziali...



➤ Shellshock consente di eseguire codice arbitrario da remoto



➤ Livello di severità

- Shellshock: 10
- Heartbleed: 5



Shellshock vs Heartbleed

Sections 

The Washington Post
Democracy Dies in Darkness

Shellshock bug could threaten millions. Compared to Heartbleed.



CENTRAL EUROPE MIDDLE EAST SCANDINAVIA AFRICA UK ITALY SPAIN MORE ▾ NEWSLETTERS ALL W

By [Gail Sullivan](#) September 26, 2014

NEW LAWSUITS THREATEN INFOSEC RESEARCH — JUST WHEN WE NEED IT MOST

Shellshock makes Heartbleed look insignificant

The new vulnerability in the Bash shell is the worst we've seen in many years. No software on critical systems can be assumed as safe.

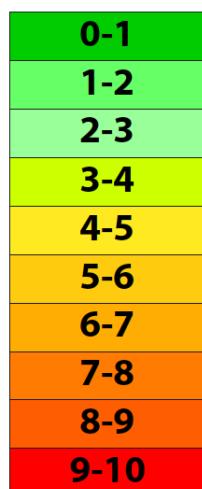


By [Larry Seltzer](#) for [Zero Day](#) | September 29, 2014 -- 11:59 GMT (12:59 BST) | Topic: [Cloud](#)



Common Vulnerability Scoring System

- IL CVE enumera le vulnerabilità, ma **non ne misura l'impatto**
 - Non stabilisce quale tra le vulnerabilità debba essere gestita più urgentemente
 - Non stabilisce come le vulnerabilità possano impattare su sistemi diversi
- Per questo motivo è stato introdotto il **Common Vulnerability Scoring System (CVSS)**
 - Stima la gravità di ogni vulnerabilità
 - Assegna ad ogni CVE un punteggio da 0 a 10
 - 0: impatto nullo
 - (0,4): impatto basso
 - [4,7]: impatto medio
 - [7,9]: impatto elevato
 - [9,10]: impatto critico



Common Vulnerability Scoring System

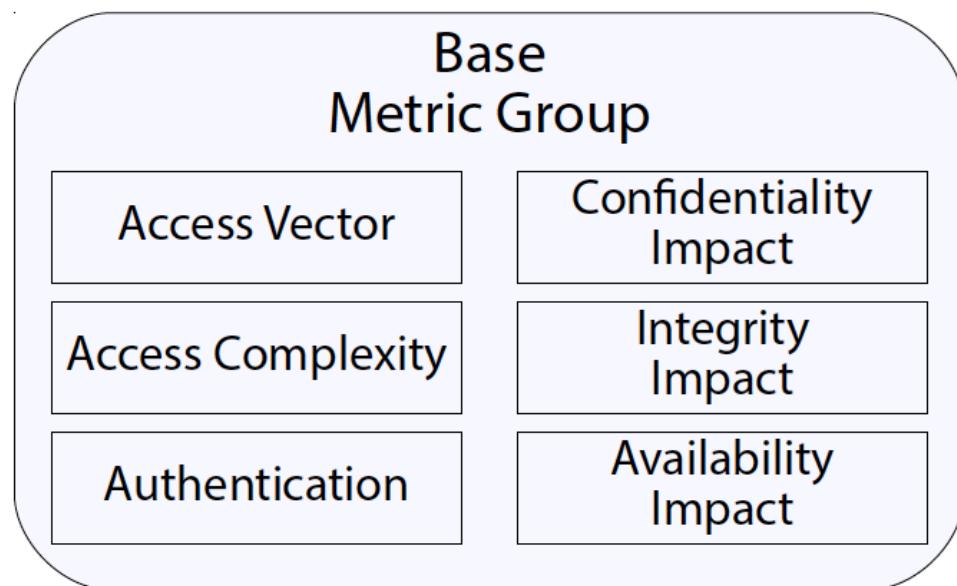
- Due versioni del CVSS sono correntemente in uso
 - Versione 2 (v2): introdotta nel 2005, pubblicata nel 2007
<https://www.first.org/cvss/v2/guide>
 - Versione 3 (v3): introdotta nel 2012, pubblicata nel 2015
<https://www.first.org/cvss/specification-document>
- Entrambe assegnano il punteggio in base a tre gruppi di metriche
 - Base (Base Metric)
 - Temporali (Temporal Metric)
 - Ambientali (Environmental Metric)



Di seguito descriviamo la versione 2

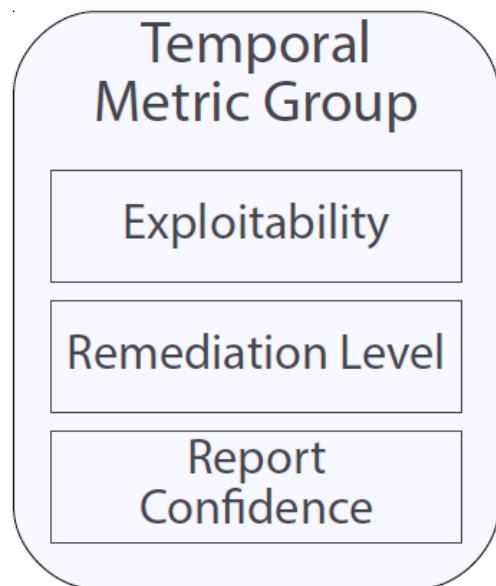
Metriche Base

- Stimano la gravità della vulnerabilità, a prescindere da fattori temporali e ambientali
 - Qual è il vettore di attacco?
 - Quanto è semplice sfruttare la vulnerabilità?
 - Qual è l'impatto sulla triade delle proprietà CIA?



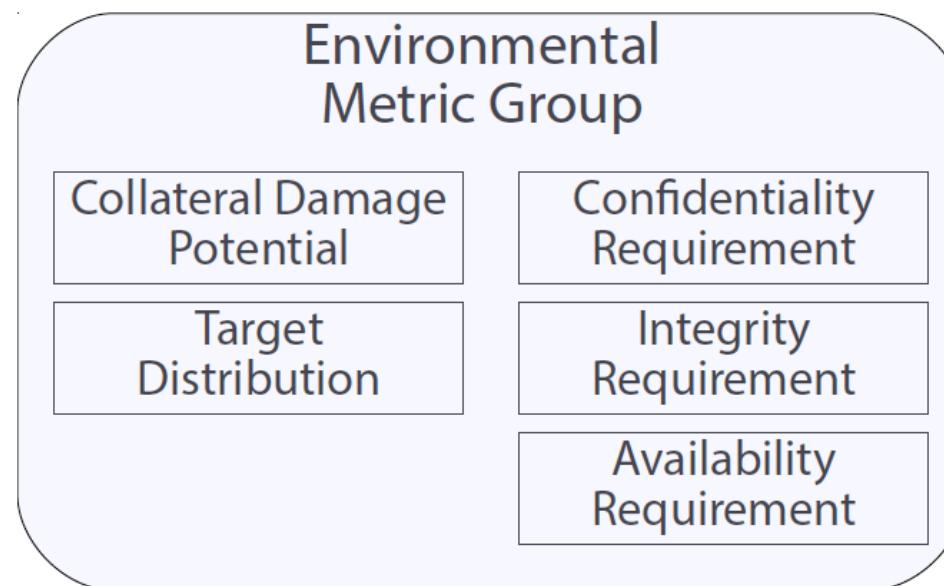
Metriche Temporali

- Stimano la gravità della vulnerabilità dal punto di vista temporale
 - E' disponibile un exploit?
 - E' disponibile una patch?



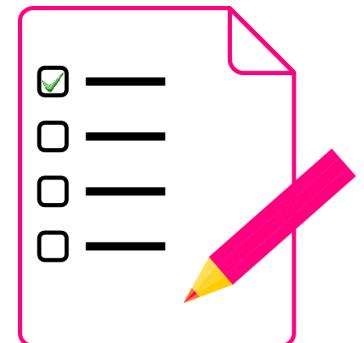
Metriche Ambientali

- Stimano la gravità della vulnerabilità dal punto di vista ambientale
 - Qual è la conseguenza di un exploit su persone e cose?
 - Quanti sistemi sono vulnerabili?



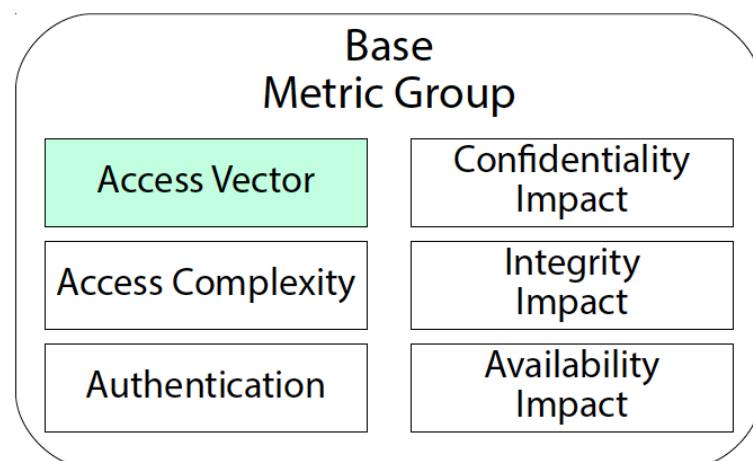
Calcolo del punteggio

- Ad ogni metrica è associata una **domanda a risposta multipla**
 - Ciascuna risposta fornisce un peso numerico
 - I singoli pesi sono poi aggregati in un risultato finale tramite una serie di formule
- Entriamo nei dettagli di ciascuna metrica e vediamo come sono associati i punteggi



Metriche Base

Tramite quale vettore di accesso può essere sfruttata la vulnerabilità?



Valore	Descrizione	Punt.
Local (L)	L'attaccante deve avere accesso fisico/un account sul sistema.	0.395
Adjacent Network (A)	L'attaccante deve avere accesso al dominio di broadcast o di collisione del sistema.	0.646
Network (N)	L'interfaccia vulnerabile è al livello 3 o superiore della pila ISO/OSI.	1.0

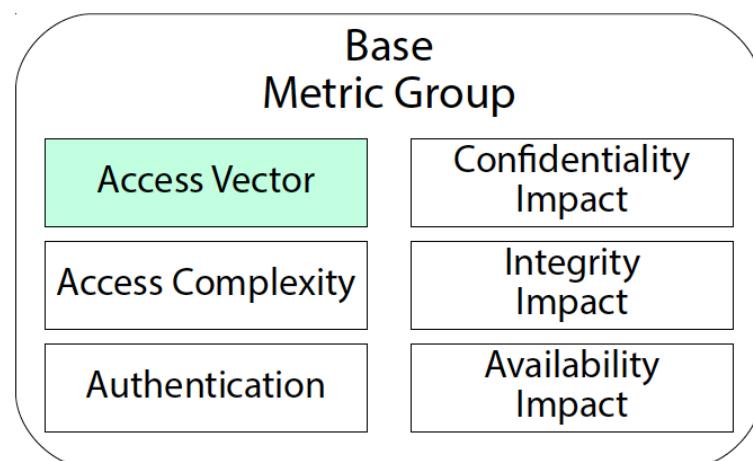
NOTA:

Alla metrica **AV (Access Vector)** può essere assegnato uno dei tre valori **L (Local)**, **A (Adjacent Network)**, **N (Network)**



Metriche Base

Tramite quale vettore di accesso può essere sfruttata la vulnerabilità?



Valore	Descrizione	Punt.
Local (L)	L'attaccante deve avere accesso fisico/un account sul sistema.	0.395
Adjacent Network (A)	L'attaccante deve avere accesso al dominio di broadcast o di collisione del sistema.	0.646
Network (N)	L'interfaccia vulnerabile è al livello 3 o superiore della pila ISO/OSI.	1.0

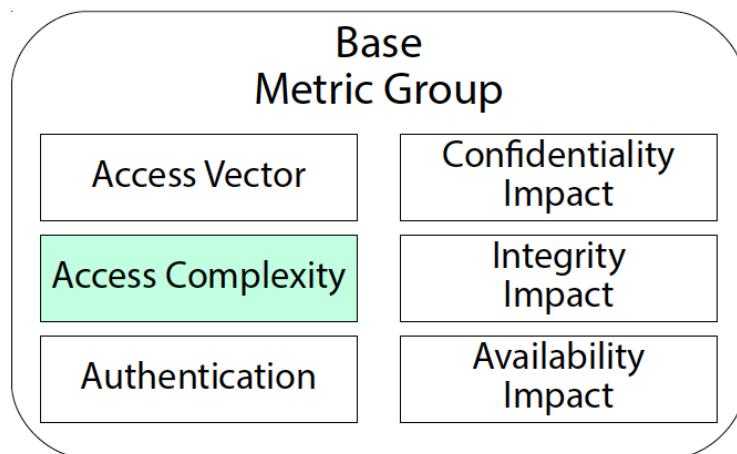
NOTA:

più alto è il punteggio parziale,
più grave è la vulnerabilità



Metriche Base

Quanto è difficile sfruttare la vulnerabilità?



Valore	Descrizione	Punt.
High (H)	Lo sfruttamento richiede condizioni particolari (corsa critica, tecniche di social engineering).	0.35
Medium (M)	Lo sfruttamento richiede alcune condizioni (ad es., configurazione non di default).	0.646
Low (L)	Lo sfruttamento non richiede nulla di particolare (funziona su sistemi standard).	1.0

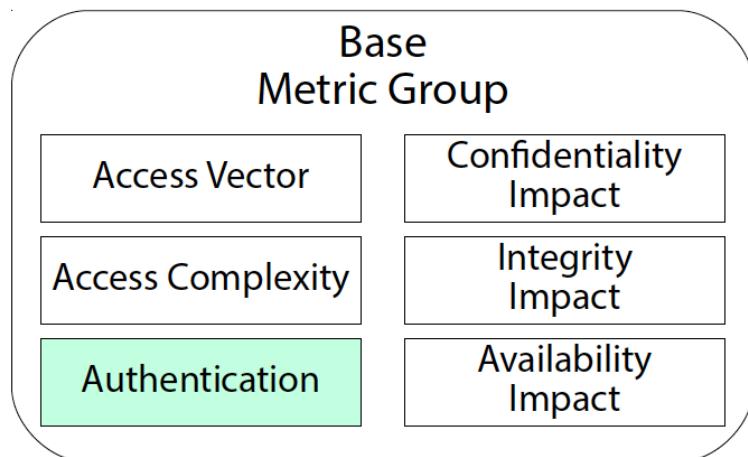
NOTA:

Alla metrica **AC** (Access Complexity) può essere assegnato uno dei tre valori **H** (High), **M** (Medium), **L** (Low)



Metriche Base

Quante volte un attaccante si deve autenticare per sfruttare la vulnerabilità?



Valore	Descrizione	Punt.
Multiple (M)	Lo sfruttamento richiede due o più autenticazioni (anche con le stesse credenziali).	0.45
Single (S)	Lo sfruttamento richiede una sola autenticazione.	0.56
None (N)	Lo sfruttamento non richiede alcuna forma di autenticazione.	0.704

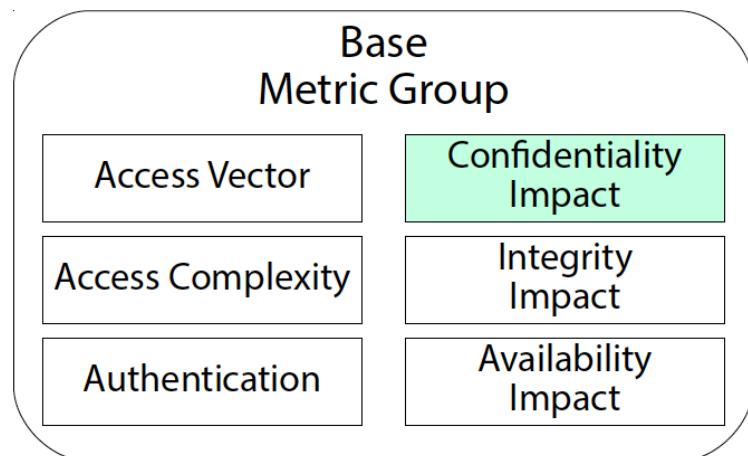
NOTA:

Alla metrica **A** (Authentication) può essere assegnato uno dei tre valori **M** (Multiple), **S** (Single), **N** (None)



Metriche Base

Qual è l'impatto della vulnerabilità
sulla confidenzialità del sistema?



Valore	Descrizione	Punt.
None (N)	Non vi è impatto alcuno.	0.0
Partial (P)	È possibile divulgare solo un sottinsieme dei dati offerti dal sistema.	0.275
Complete (C)	È possibile divulgare l'intero insieme dei dati offerti dal sistema.	0.660

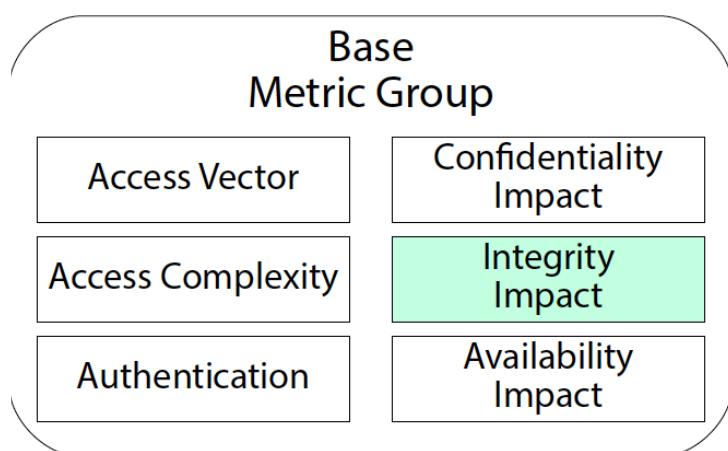
NOTA:

Alla metrica **CI** (Confidentiality Impact) può essere assegnato uno dei tre valori **N** (None), **P** (Partial), **C** (Complete)



Metriche Base

Qual è l'impatto della vulnerabilità
sull'integrità del sistema?



Valore	Descrizione	Punt.
None (N)	Non vi è impatto alcuno.	0.0
Partial (P)	È possibile modificare solo un sottinsieme dei dati offerti dal sistema.	0.275
Complete (C)	È possibile modificare l'intero insieme dei dati offerti dal sistema.	0.660

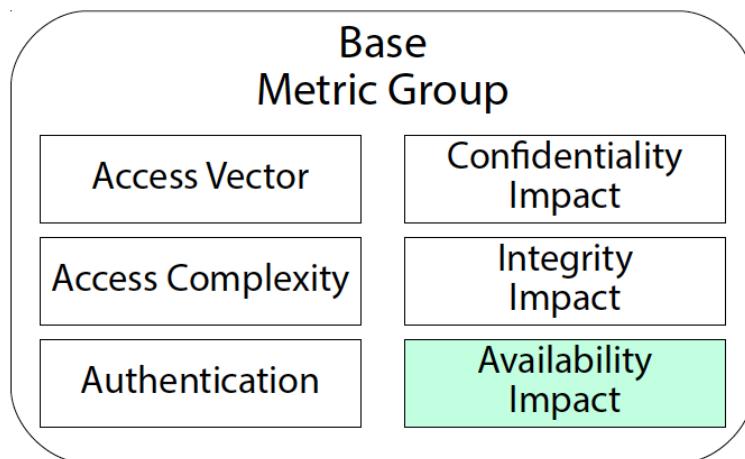
NOTA:

Alla metrica **II (Integrity Impact)** può essere assegnato uno dei tre valori **N (None)**, **P (Partial)**, **C (Complete)**



Metriche Base

Qual è l'impatto della vulnerabilità
sulla disponibilità del sistema?



Valore	Descrizione	Punt.
None (N)	Non vi è impatto alcuno.	0.0
Partial (P)	È possibile ridurre parzialmente le prestazioni e/o le funzioni offerte dal sistema.	0.275
Complete (C)	È possibile ridurre completamente le prestazioni e/o le funzioni offerte dal sistema.	0.660

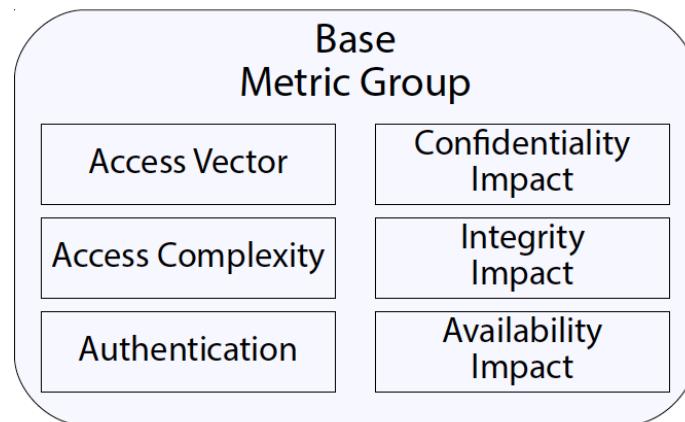
NOTA:

Alla metrica **AI** (Availability Impact) può essere assegnato uno dei tre valori **N** (None), **P** (Partial), **C** (Complete)



Metriche Base

- Le risposte relative alle metriche base sono presentate sotto forma di stringa di testo
- Tale stringa, detta **vector string**, è formata da coppie di abbreviazioni **metrica:risposta** separate dal carattere /
 - Esempio: AV:N/AC:L/Au:N/C:P/I:P/A:C



Calcolo del Punteggio Base

Il **Punteggio Base** stima la gravità della vulnerabilità
senza considerare fattori temporali ed ambientali

$$\text{Exploitability} = 20 * \text{AccessVector} * \text{AccessComplexity} * \text{Authentication}$$

$$\text{Impact} = 10.41 * (1 - (1 - \text{ConfImpact}) * (1 - \text{IntegImpact}) * (1 - \text{AvailImpact}))$$

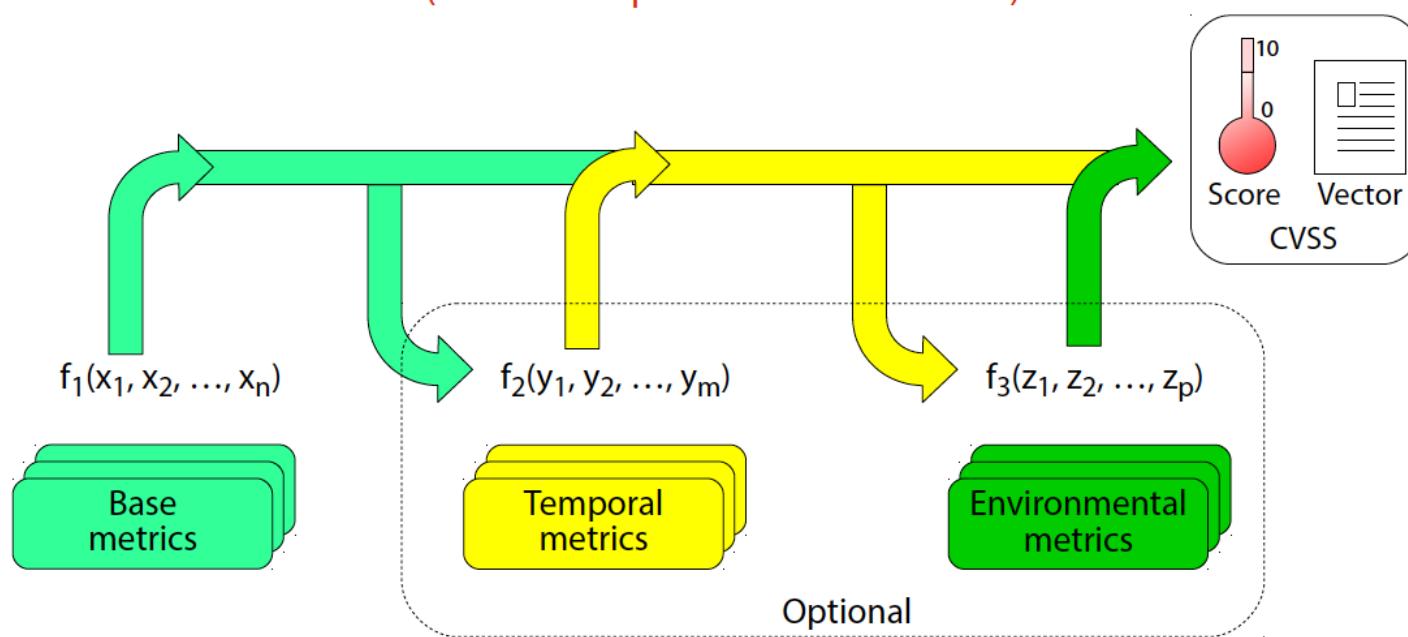
$$f(\text{Impact}) = \begin{cases} 0 & \text{if Impact} = 0 \\ 1.176 & \text{otherwise} \end{cases}$$

$$\text{BaseScore} = \text{roundTo1Decimal} (((0.6 * \text{Impact}) + (0.4 * \text{Exploitability}) - 1.5) * f(\text{Impact}))$$



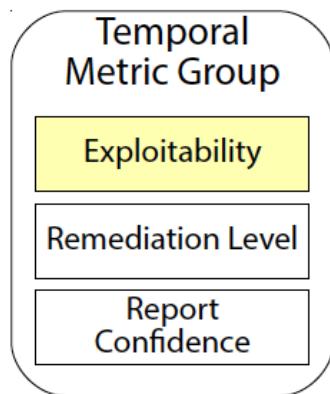
Altri punteggi

- I punteggi associati alle altre due metriche sono opzionali
 - Si calcolano nello stesso modo (con questionari diversi)
- Relazioni tra i punteggi
 - Il Punteggio **Temporale** ingloba il Punteggio **Base**
 - Il Punteggio **Ambientale** ingloba il Punteggio **Temporale**



Metriche Temporali

Qual è lo stato attuale delle tecniche di sfruttamento della vulnerabilità ?



Valore	Descrizione	Punt.
Unproven (U)	L'exploit non è pubblico, oppure esiste in linea solo teorica.	0.85
Proof of Concept (P)	È disponibile una bozza dimostrativa (Proof of Concept, PoC). Richiede adattamenti non banali per funzionare.	0.9
Functional (F)	È disponibile un exploit funzionante nella maggioranza dei casi in cui la vulnerabilità è presente.	0.95
High (H)	La vulnerabilità può essere sfruttata in modo automatico (anche da worm e virus).	1.0
Not Defined (ND)	Si ignori tale punteggio.	1.0

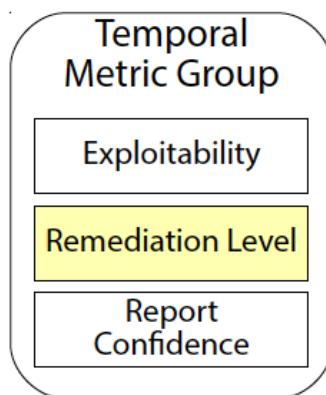
NOTA:

Alla metrica **E (Exploitability)** può essere assegnato uno dei cinque valori **U (Unproven)**, **P (Proof of Concept)**, **F (Functional)**, **H (High)**, **ND (Not Defined)**



Metriche Temporali

E' presente un rimedio per mitigare la vulnerabilità ?



Valore	Descrizione	Punt.
Official fix (O)	Il vendor mette a disposizione un rimedio ufficiale (patch, aggiornamento software).	0.87
Temporary fix (T)	Il vendor mette a disposizione un rimedio ufficiale, ma temporaneo.	0.90
Workaround (W)	Una terza parte (NON il vendor) mette a disposizione un rimedio non ufficiale.	0.95
Unavailable (U)	Non è disponibile un rimedio, o è impossibile applicare una soluzione suggerita.	1.0
Not Defined (ND)	Si ignori tale punteggio.	1.0

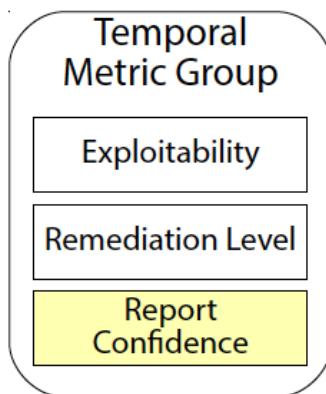
NOTA:

Alla metrica **RL** (Remediation Level) può essere assegnato uno dei cinque valori **O** (Official fix), **T** (Temporary fix), **W** (Workaround), **U** (Unaivalable), **ND** (Not Defined)



Metriche Temporali

La vulnerabilità esiste veramente?
E' descritta in maniera credibile?



Valore	Descrizione		Punt.
Unconfirmed (UC)	La vulnerabilità è divulgata da una singola fonte non confermata, o da più fonti in mutuo conflitto.		0.9
Uncorroborated (UR)	La vulnerabilità è divulgata da più fonti concordi. Può esistere un livello residuo di incertezza.		0.95
Confirmed (C)	La vulnerabilità è confermata dal vendor.		1.0
Not Defined (ND)	Si ignori tale punteggio.		1.0

NOTA:

Alla metrica **RC** (Report Confidence) può essere assegnato uno dei quattro valori **UC** (Unconfirmed), **UR** (Uncorroborated), **C** (Confirmed), **ND** (Not Defined)



Calcolo del Punteggio Temporale

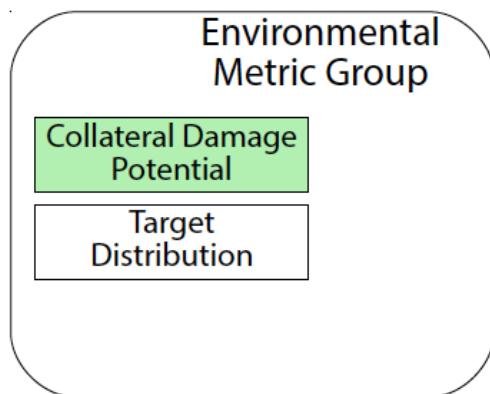
Il **Punteggio Temporale** stima la gravità della vulnerabilità includendo il fattore temporale

$$\text{TemporalScore} = \text{roundTo1 Decimal} (\text{BaseScore} * \text{Exploitab} * \text{RemedLvl} * \text{ReportConf})$$



Metriche Ambientali

Qual è l'impatto della vulnerabilità sui sistemi fisici,
sulle persone e sulle risorse finanziarie ?



Valore	Descrizione	Punt.
None (N)	Nessun impatto.	0
Low (L)	Danno fisico basso, perdita marginale di guadagno.	0.1
Low-Medium (LM)	Danno fisico ed economico moderato.	0.3
Medium-High (MH)	Danno fisico ed economico significativo.	0.4
High (H)	Danno fisico ed economico catastrofico.	0.5
Not Defined (ND)	Si ignori tale punteggio.	1.0

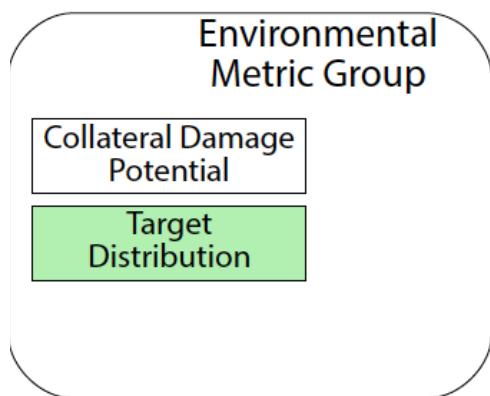
NOTA:

Alla metrica **CDP** (Collateral Damage Potential) può essere assegnato uno dei sei valori **N** (None), **L** (Low), **LM** (Low-Medium), **MH** (Medium-High), **H** (High), **ND** (Not Defined)



Metriche Ambientali

Quale percentuale di asset
è soggetta alla vulnerabilità ?



Valore	Descrizione	Punt.
None (N)	Percentuale nulla.	0
Low (L)	1%-25% degli asset.	0.25
Medium (M)	26%-75% degli asset.	0.75
High (H)	76%-100% degli asset.	1.0
Not Defined (ND)	Si ignori tale punteggio.	1.0

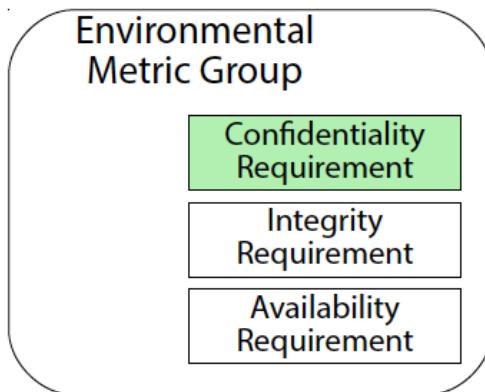
NOTA:

Alla metrica TD (Target Distribution) può essere assegnato uno dei cinque valori N (None), L (Low), M (Medium), H (High), ND (Not Defined)



Metriche Ambientali

Qual è l'impatto di una
perdita di confidenzialità?



Valore	Descrizione	Punt.
Low (L)	L'impatto è lieve.	0.5
Medium (M)	L'impatto è serio.	1.0
High (H)	L'impatto è catastrofico.	1.51
Not Defined (ND)	Si ignori tale punteggio.	1.0

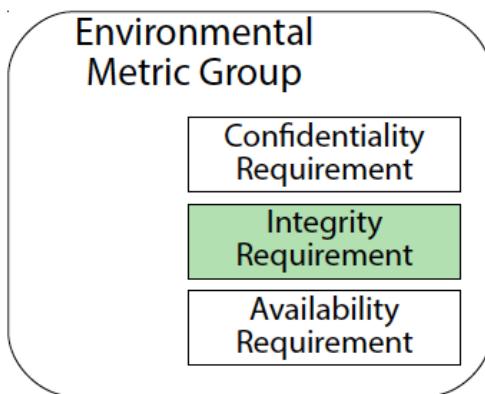
NOTA:

Alla metrica **CR** (Confidentiality Requirement) può essere
assegnato uno dei quattro valori
L (Low), **M (Medium)**, **H (High)**, **ND (Not Defined)**



Metriche Ambientali

Qual è l'impatto di una perdita di integrità?



Valore	Descrizione	Punt.
Low (L)	L'impatto è lieve.	0.5
Medium (M)	L'impatto è serio.	1.0
High (H)	L'impatto è catastrofico.	1.51
Not Defined (ND)	Si ignori tale punteggio.	1.0

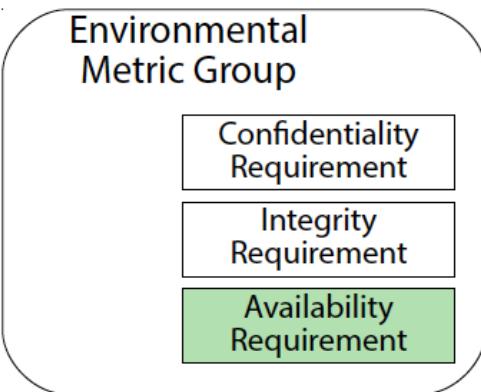
NOTA:

Alla metrica **IR** (Integrity Requirement) può essere assegnato uno dei quattro valori
L (Low), **M** (Medium), **H** (High), **ND** (Not Defined)



Metriche Ambientali

Qual è l'impatto di una perdita di disponibilità?



Valore	Descrizione	Punt.
Low (L)	L'impatto è lieve.	0.5
Medium (M)	L'impatto è serio.	1.0
High (H)	L'impatto è catastrofico.	1.51
Not Defined (ND)	Si ignori tale punteggio.	1.0

NOTA:

Alla metrica **AR** (Availability Requirement) può essere assegnato uno dei quattro valori **L (Low)**, **M (Medium)**, **H (High)**, **ND (Not Defined)**



Calcolo del Punteggio Ambientale

Il Punteggio Ambientale stima la gravità della vulnerabilità includendo il fattore ambientale

$$AdjImp = \min(10, 10.41 * (1 - (1 - ConfImp * ConfReq) * (1 - IntImp * IntReq) * (1 - AvImp * AvReq)))$$

AdjTemp = punteggio Temporal ricalcolato con AdjImp al posto di Impact

*EnvironmentalScore = roundTo1 Decimal ((AdjTemp + (10 - AdjTemp) * CollatDamPot) * TargetDist)*



Punteggio CVSS

➤ Chi calcola i punteggi CVSS?

- I **Punteggi Base e Temporale** sono calcolati da venditori di software
- Il **Punteggio Ambientale** è calcolato dagli amministratori delle infrastrutture



➤ Chi utilizza i punteggi CVSS?

- I punteggi sono utilizzati da chiunque abbia a che fare con il processo di gestione della sicurezza

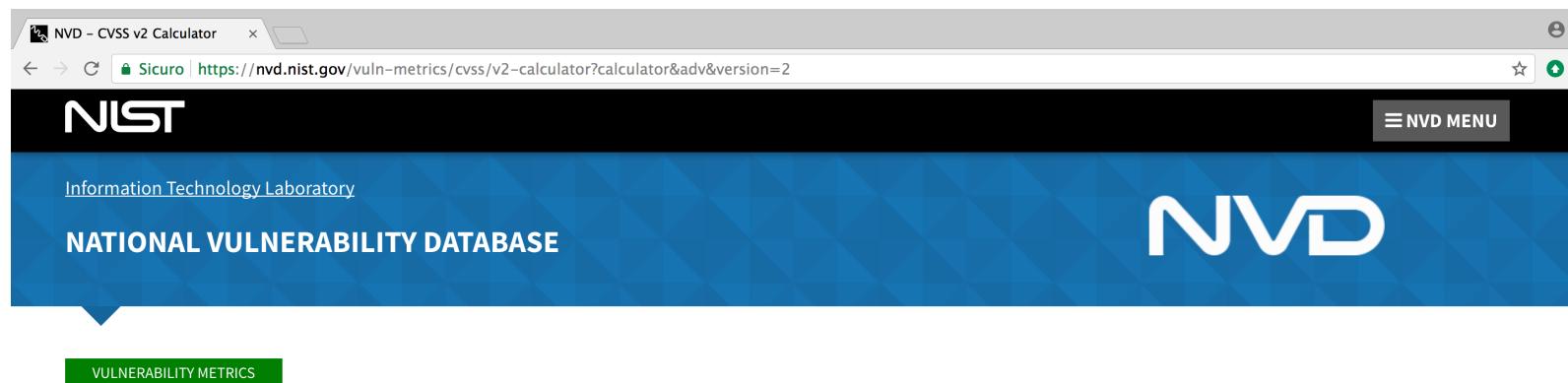


Foglio di calcolo CVSS v2

Al seguente URL

<https://nvd.nist.gov/cvss.cfm?calculator&adv&version=2>

è presente un foglio di calcolo Web che consente di calcolare i punteggi CVSS v2 con pochi click



Common Vulnerability Scoring System Calculator Version 2

This page shows the components of the [CVSS](#) score for example and allows you to refine the CVSS base score. Please read the [CVSS standards guide](#) to fully understand how to score CVSS vulnerabilities and to interpret CVSS scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.



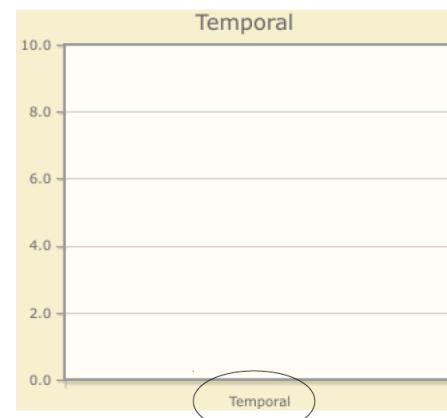
Foglio di calcolo CVSS v2

- La parte iniziale della pagina Web mostra i diagrammi a barre dei vari punteggi

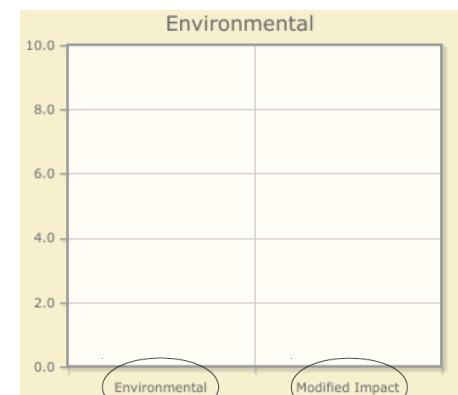


Punteggio
Base

Metriche usate per
calcolare Base



Punteggio
Temporal



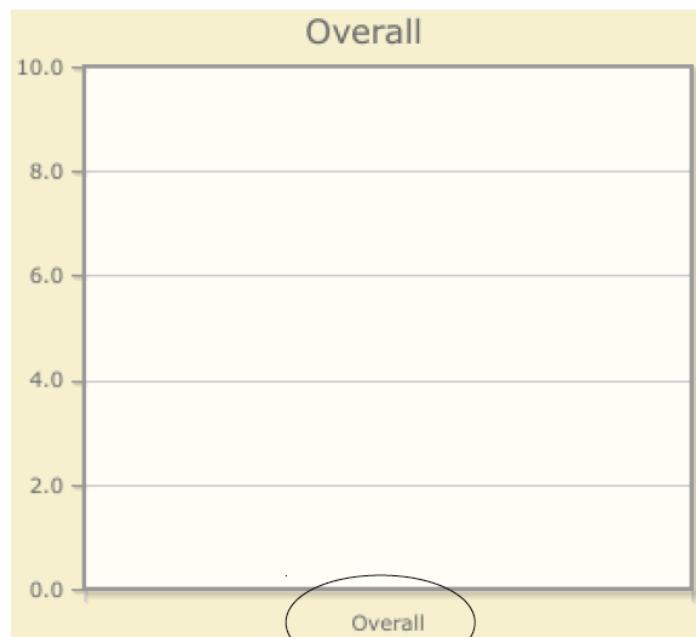
Punteggio
Environmental

Metrica usata per
calcolare
Environmental



Foglio di calcolo CVSS v2

- L'ultimo diagramma riporta il punteggio finale (Overall): corrisponde al punteggio che si è deciso di calcolare



CVSS Base Score	0
Impact Subscore	0
Exploitability Subscore	0
CVSS Temporal Score	0
CVSS Environmental Score	0
Modified Impact Subscore	0
Overall CVSS Score	0
<u>Show Equations</u>	

Scheda riassuntiva



Base, Temporal
o Environmental

Foglio di calcolo CVSS v2

- Sotto la scheda riassuntiva sono presenti tre tab per l'immissione delle scelte possibili
- Il primo tab è relativo alle **Metriche Base**

▼ **Base Score Metrics**

Exploitability Metrics			Impact Metrics		
Access Vector (AV)*			Confidentiality Impact (C)*		
Local (AV:L)	Adjacent Network (AV:A)	Network (AV:N)	None (C:N)	Partial (C:P)	Complete (C:C)
Access Complexity (AC)*			Integrity Impact (I)*		
High (AC:H)	Medium (AC:M)	Low (AC:L)	None (I:N)	Partial (I:P)	Complete (I:C)
Authentication (Au)*			Availability Impact (A)*		
Multiple (Au:M)	Single (Au:S)	None (Au:N)	None (A:N)	Partial (A:P)	Complete (A:C)

* - All base metrics are required to generate a base score.



Foglio di calcolo CVSS v2

➤ Il secondo tab è relativo alle **Metriche Temporali**

Temporal Score Metrics					
Exploitability (E)	Not Defined (E:ND)	Unproven that exploit exists (E:U)	Proof of concept code (E:POC)	Functional exploit exists (E:F)	High (E:H)
Remediation Level (RL)	Not Defined (RL:ND)	Official fix (RL:OF)	Temporary fix (RL:TF)	Workaround (RL:W)	Unavailable (RL:U)
Report Confidence (RC)	Not Defined (RC:ND)	Unconfirmed (RC:UC)	Uncorroborated (RC:UR)	Confirmed (RC:C)	

➤ Il terzo tab è relativo alle **Metriche Ambientali**

Environmental Score Metrics					
General Modifiers			Impact Subscore Modifiers		
Collateral Damage Potential (CDP)			Confidentiality Requirement (CR)		
Not Defined (CDP:ND) None (CDP:N) Low (light loss) (CDP:L) Low-Medium (CDP:LM) Medium-High (CDP:MH) High (catastrophic loss) (CDP:H)			Not Defined (CR:ND) Low (CR:L) Medium (CR:M) High (CR:H)		
Target Distribution (TD)			Integrity Requirement (IR)		
Not Defined (TD:ND) None [0%] (TD:N) Low [0-25%] (TD:L) Medium [26-75%] (TD:M) High [76-100%] (TD:H)			Not Defined (IR:ND) Low (IR:L) Medium (IR:M) High (IR:H)		
Availability Requirement (AR)			Not Defined (AR:ND) Low (AR:L) Medium (AR:M) High (AR:H)		



Un esempio concreto

- Si consideri un'azienda che offre i propri prodotti al pubblico mediante un server Web che fornisce
 - Un catalogo dei prodotti
 - Un negozio elettronico



- Il Web server è vulnerabile a **CVE-2014-6271**
- Si vuole calcolare il **Punteggio Ambientale CVSS v2** relativo a tale vulnerabilità



Un esempio concreto

➤ Iniziamo a considerare le **Metriche Base**

- Il Web server è accessibile pubblicamente tramite Internet, quindi **AV:N**
- Il Web server è vulnerabile nella sua configurazione di default, quindi **AC:L**
- Lo sfruttamento non richiede alcuna autenticazione, quindi **Au:N**



Exploitability Metrics

Access Vector (AV)*

Local (AV:L) **Adjacent Network (AV:A)** **Network (AV:N)**

Access Complexity (AC)*

High (AC:H) **Medium (AC:M)** **Low (AC:L)**

Authentication (Au)*

Multiple (Au:M) **Single (Au:S)** **None (Au:N)**



Un esempio concreto

➤ Continuiamo con le **Metriche Base**

- Il Web server esegue con un utente avente privilegi ridotti
- Il database back-end associato al Web server non memorizza tutte le informazioni aziendali
- Pertanto, l'impatto sulle proprietà della triade CIA è parziale

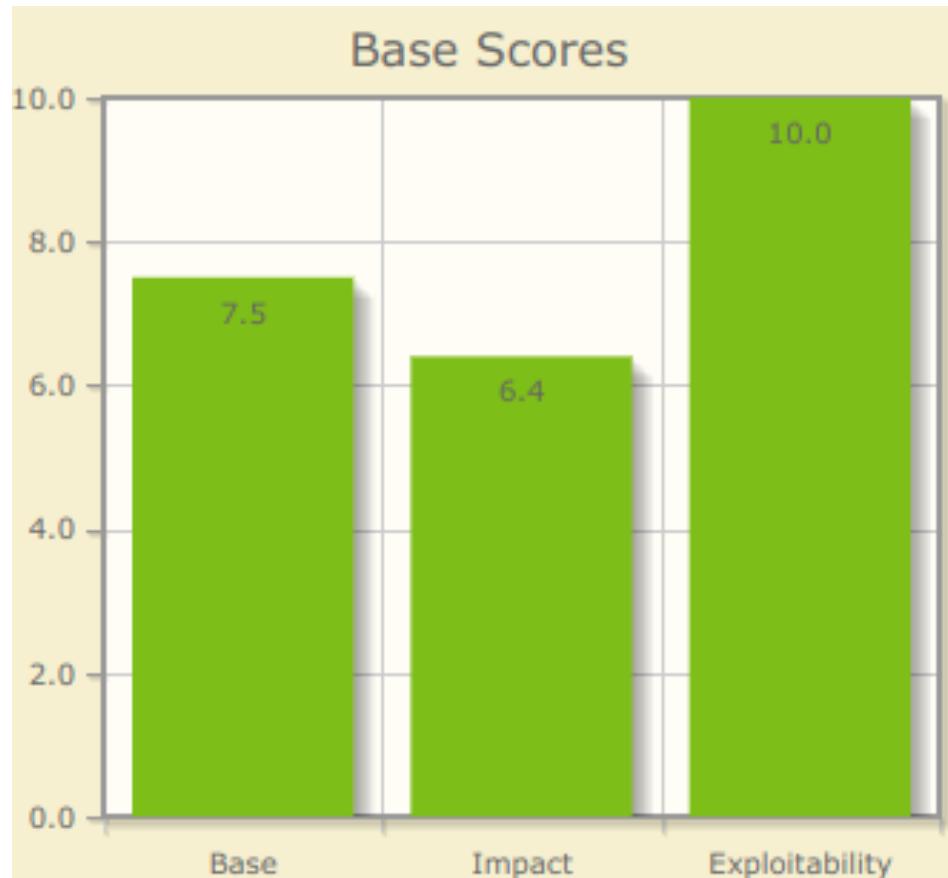


Impact Metrics		
Confidentiality Impact (C)*		
None (C:N)	Partial (C:P)	Complete (C:C)
Integrity Impact (I)*		
None (I:N)	Partial (I:P)	Complete (I:C)
Availability Impact (A)*		
None (A:N)	Partial (A:P)	Complete (A:C)



Un esempio concreto

➤ Otteniamo il **Punteggio Base**



CVSS Base Score	7.5
Impact Subscore	6.4
Exploitability Subscore	10
CVSS Temporal Score	NaN
CVSS Environmental Score	NaN
Modified Impact Subscore	NaN
Overall CVSS Score	NaN
<u>Show Equations</u>	



Un esempio concreto

➤ Passiamo a considerare le **Metriche Temporali**

- Sono disponibili script per l'esecuzione dell'exploit, quindi **E:H**
- E' stata rilasciata una nuova versione di BASH che elimina il difetto, quindi **RL:OF**
- La vulnerabilità è vera, quindi **RC:C**

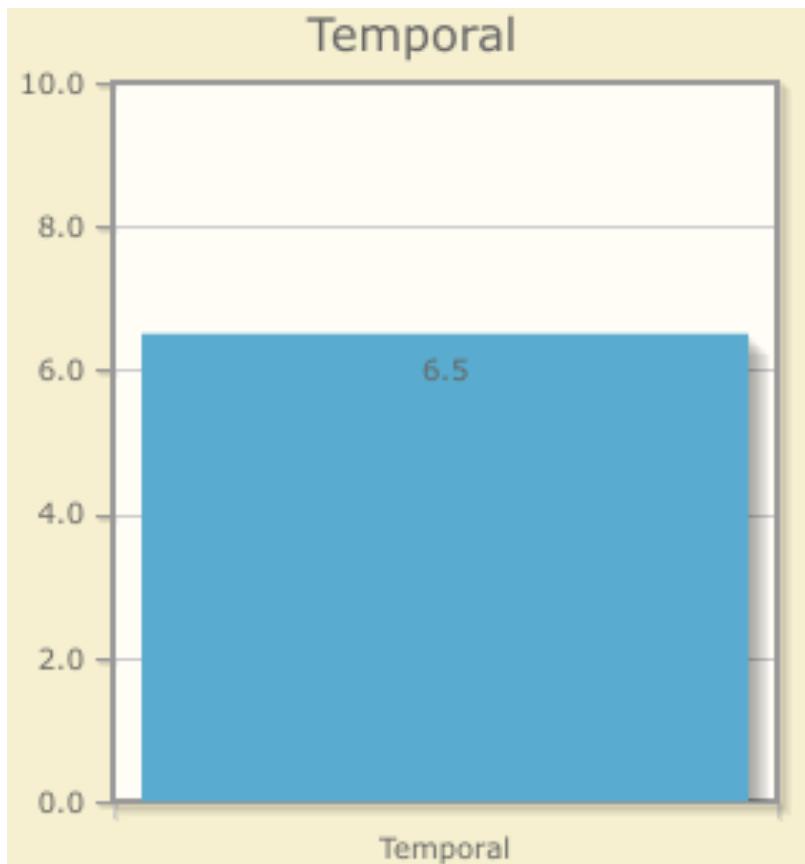


Exploitability (E)				
Not Defined (E:ND)	Unproven that exploit exists (E:U)	Proof of concept code (E:POC)	Functional exploit exists (E:F)	High (E:H)
Remediation Level (RL)				
Not Defined (RL:ND)	Official fix (RL:OF)	Temporary fix (RL:TF)	Workaround (RL:W)	Unavailable (RL:U)
Report Confidence (RC)				
Not Defined (RC:ND)	Unconfirmed (RC:UC)	Uncorroborated (RC:UR)	Confirmed (RC:C)	



Un esempio concreto

➤ Otteniamo il **Punteggio Temporale**



CVSS Base Score	7.5
Impact Subscore	6.4
Exploitability Subscore	10
CVSS Temporal Score	6.5
CVSS Environmental Score	NaN
Modified Impact Subscore	NaN
Overall CVSS Score	NaN
<u>Show Equations</u>	



Un esempio concreto

➤ Continuiamo con le **Metriche Ambientali**

- Il danno massimo stimato sul Web server è un DoS che può rendere molto lento il negozio, quindi **CDP: MH**
- Il Web server è l'unico asset soggetto a CVE-2014-6271, quindi **TD:L**



General Modifiers

Collateral Damage Potential (CDP)

Not Defined (CDP:ND)	None (CDP:N)	Low (light loss) (CDP:L)	Low-Medium (CDP:LM)	Medium-High (CDP:MH)	High (catastrophic loss) (CDP:H)
----------------------	--------------	--------------------------	---------------------	----------------------	----------------------------------

Target Distribution (TD)

Not Defined (TD:ND)	None [0%] (TD:N)	Low [0-25%] (TD:L)	Medium [26-75%] (TD:M)	High [76-100%] (TD:H)
---------------------	------------------	--------------------	------------------------	-----------------------



Un esempio concreto

➤ Continuiamo con le **Metriche Ambientali**

- Il Web server esegue con un utente non privilegiato
- Il database back-end associato al Web server non memorizza tutte le informazioni aziendali
- Pertanto, **CR:M, IR:M, AR:M**



Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:ND)	Low (CR:L)	Medium (CR:M)	High (CR:H)
---------------------	------------	---------------	-------------

Integrity Requirement (IR)

Not Defined (IR:ND)	Low (IR:L)	Medium (IR:M)	High (IR:H)
---------------------	------------	---------------	-------------

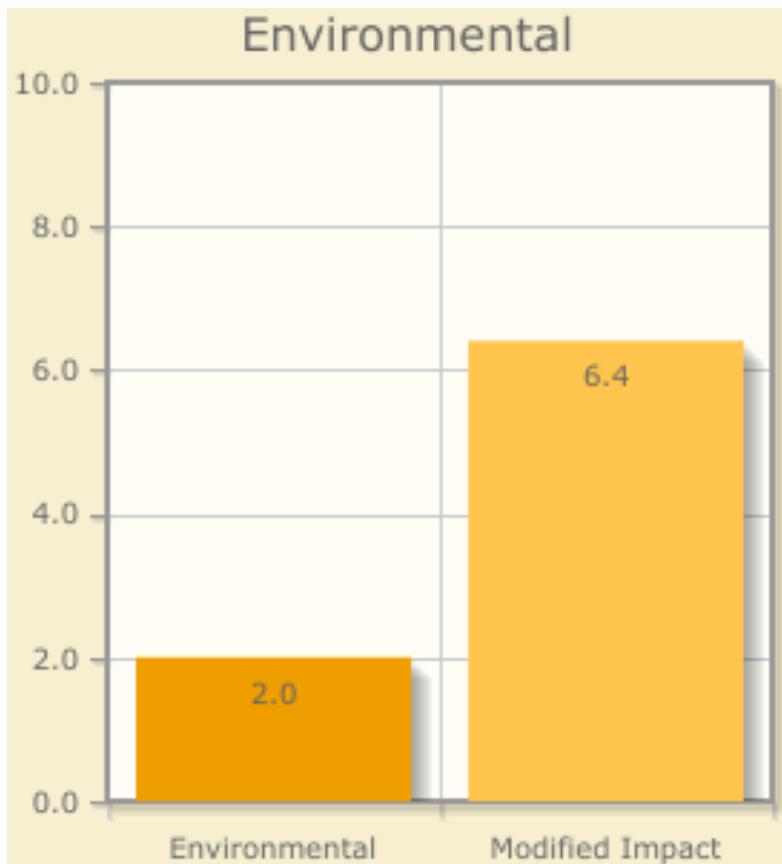
Availability Requirement (AR)

Not Defined (AR:ND)	Low (AR:L)	Medium (AR:M)	High (AR:H)
---------------------	------------	---------------	-------------



Un esempio concreto

➤ Otteniamo il **Punteggio Ambientale**



CVSS Base Score	7.5
Impact Subscore	6.4
Exploitability Subscore	10
CVSS Temporal Score	6.5
CVSS Environmental Score	2
Modified Impact Subscore	6.4
Overall CVSS Score	2
Show Equations	



Un esempio concreto

➤ Notiamo che, per l'esempio considerato, il Punteggio Temporale è più basso del Punteggio Base

➤ Esiste una patch ufficiale contro la vulnerabilità

➤ Inoltre, il Punteggio Ambientale è più basso del Punteggio Temporale

➤ Sostanzialmente, si tratta di danni locali



NOTA:

C'è da osservare che le risposte ai questionari sono soggettive

