



Measuring Security Risks with CVSS

Eugene Teo, GCIH, RHCA, RHCSS
Red Hat Security Response Team
eugene@{redhat.com,kernel.sg}
2010-03-05

Background

- IT management not getting easier
- End user, server environment
- Hardware and software
- Updates and security fixes
- Patch management policy? Good?
- Understand security flaws? Affect your environment?
- What do vendors do?
- What are the problems?



Different vulnerability scoring systems

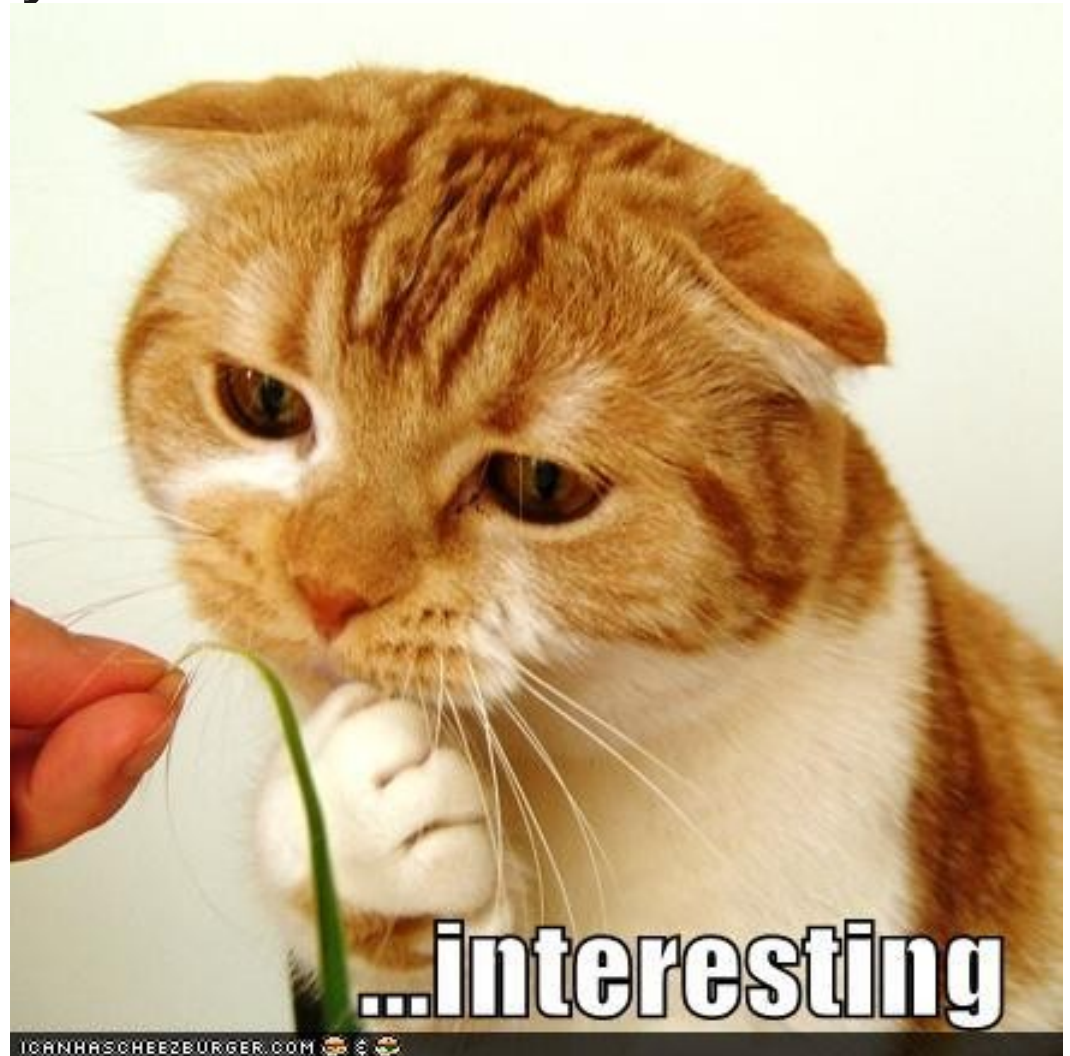
- CERT/CC vulnerability metric
- NVD severity indices
- Microsoft severity rating system
- Red Hat severity ratings
- Novell vulnerability severity classification
- etc





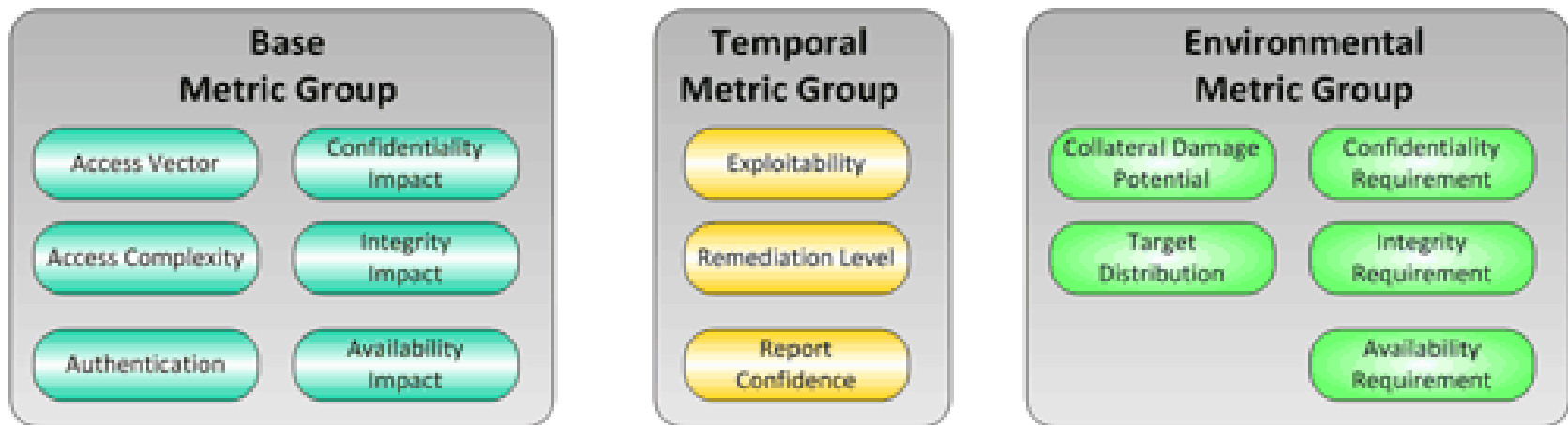
Purpose of CVSS

- Standardized Vulnerability Scores
- Open Framework
- Prioritized Risk



CVSS

- Composed of 3 metric groups
- Base
- Temporal (optional)
- Environmental (optional)



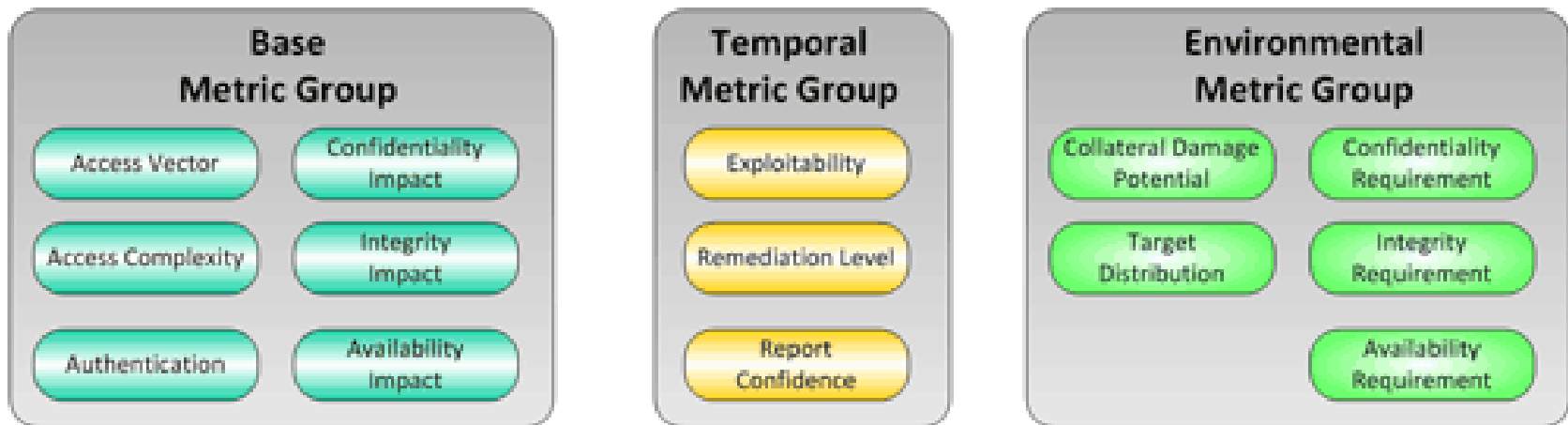
How CVSS works?

- Base metrics assigned values
- Equation calculates score 0 (no risk) to 10 (high risk)
- Creates vector
- Can be refined with temporal and environmental metrics but not required



Who does the scoring?

- Base and temporal metrics – vulnerability bulletin analysts, security product vendors, application vendors, etc
- Environmental metrics - end-users



Base metrics group

- CVSS base metrics group covers the constant aspects of a given vulnerability using six measurements:
 - Access Vector (**AV**)
Local, Adjacent Network, Network
 - Access Complexity (**AC**)
High, Medium, Low
 - Authentication (**Au**)
Multiple, Single, None
 - Confidentiality (**C**)
 - Integrity (**I**)
 - Availability (**A**)
- None, Partial, Complete**



Examples - CVE-2006-6304

- Rewrite attack flaw in `do_coredump()` of Linux kernel
- Local attacker leveraging this flaw to guess the file name a process is going to dump its core to, prior to process crashing, could use this append data to dumped core file
- Only on systems with `fs.suid_dumpable = 2` (default 0)
- Base vector is `AV:L/AC:M/Au:N/C:N/I:P/A:N`
- Metrics result in base score of 1.9 (Low)



Examples - CVE-2009-2698

- Vulnerability related to how Linux kernel handles MSG_MORE flag on UDP sockets
- Successful exploit can trigger a NULL pointer dereference, leading to a local denial of service or privilege escalation
- Base vector is AV:L/AC:L/Au:N/C:C/I:C/A:C
- Metrics result in base score of 7.2 (Important)



Examples - CVE-2010-0408

- `mod_proxy_ajp` would return the wrong status code if it encountered an error causing a backend server to be put into an error state until the retry timeout expired. A remote attacker could send malicious requests to trigger this issue, resulting in a denial of service
- Base vector is `AV:N/AC:L/Au:N/C:N/I:N/A:P`
- Metrics result in base score of 5 (Moderate)



Examples - CVE-2009-4212

- `% ps aux|grep kdc`
root 8370 0.0 0.0 62672 2320 ? Ss Feb20
0:04 /usr/kerberos/sbin/krb5kdc
- Multiple integer underflow flaws, leading to heap-based corruption found in MIT Kerberos Key Distribution Center (KDC). If a remote KDC client were able to provide a specially-crafted AES- or RC4-encrypted ciphertext or texts, it could potentially lead to either a denial of service of the central KDC, or arbitrary code execution with the privileges of the KDC (root privs)
- Base vector is AV:N/AC:L/Au:N/C:C/I:C/A:C
- Metrics result in base score of 10 (Critical)



Open source software

- CVSS v2 may vary for each vendor's version, depending on
 - Version they ship
 - How they ship it
 - What platform
 - How it is compiled
- Use CVSS v2 base score provided by vendor when available in preference to score from third-party



Red Hat and CVSS

- Involved in CVSS for several years
- Evaluated how it can be used with open source software
- Helped with corrections to scores given by National Vulnerability Database (NVD)
- Besides existing severity ratings, provided CVSS v2 base metrics for all 2009 vulnerabilities



Red Hat and CVSS

https://www.redhat.com/security/data/cve/CVE-2010-0291.html

redhat.

Security Response Team

2010 CVE

CVE-2010-0291

2009 CVE

2008 CVE

2007 CVE

2006 CVE

2005 CVE

2004 CVE

2003 CVE

2002 CVE

2001 CVE

2000 CVE

1999 CVE

CVE-2010-0291

Impact: Important ([classification](#))

Public: December 07 2009

Bugzilla: [556703](#): CVE-2010-0291 kernel: untangle the do_mremap()

Details

The MITRE CVE dictionary describes this issue as:

The Linux kernel before 2.6.32.4 allows local users to gain privileges or cause a denial of service (panic) by calling the (1) mmap or (2) mremap function, aka the "do_mremap() mess" or "mremap/mmap mess."

Find out more about CVE-2010-0291 from the [MITRE CVE dictionary](#) and [NIST NVD](#).

CVSS v2 metrics

Base Score:	7.2	Base Metrics:	AV:L/AC:L/Au:N/C:C/I:C/A:C
Access Vector:	Local	Confidentiality Impact:	Complete
Access Complexity:	Low	Integrity Impact:	Complete
Authentication:	None	Availability Impact:	Complete

Find out more about [Red Hat support for the Common Vulnerability Scoring System \(CVSS\)](#).



Find out more

- Now you have an idea what CVSS is and how to interpret CVSS v2 base metrics
- Learn more at:
 - <http://www.first.org/cvss/cvss-guide.html#i2.2.1>
 - <http://www.redhat.com/security/updates/cvss/>
 - <http://www.redhat.com/security/data/cve/>



secalert@redhat.com

- Address used to ask security vulnerability related questions
 - Reporting new vulnerabilities
 - Asking how we addressed various vulnerabilities
 - Charter to respond within 3 business days

99%

secalert@redhat.com mails had first response within one business day, Feb 2009- Mar 2010



References

- <http://icanhascheezburger.files.wordpress.com>
- <http://www.redhat.com/security/updates/classification/>
- <http://www.microsoft.com/technet/security/bulletin/rating.msp>
- <http://nvd.nist.gov/cvss.cfm>
- <https://www.kb.cert.org/vuls/html/fieldhelp>
- <http://www.suse.de/~thomas/papers/Severity-Metric.pdf>

